A **CRC Press** FREEBOOK

Security, Audit and Leadership Series

Risk and Privacy FREE BOOK

CRC Press
Taylor & Francis Group

TABLE OF CONTENTS

Security, Audit and Leadership Series
The books included above are part of the CRC Press Security, Audit and Leadership series. The fundamental goal of this exciting series is to produce leading-edge books on critical subjects facing security and audit executives and practitioners.
Key topics addressed include Leadership, Cybersecurity, Security Leadership, Privacy, Strategic Risk Management, Auditing IT, Audit Management and Leadership, and Operational Auditing.

To see the full series of books, go to: https://www.routledge.com/Security-Audit-and-Leadership-Series/book-series/CRCINTAUDITA

SECURITY, AUDIT AND LEADERSHIP SERIES

Security Risk Management - The Driving Force for Operational Resilience

The Firefighting Paradox

Jim Seaman and Michael Gioia

CRC Press
Taylor & Francis Group

Security Risk Management – The Driving Force for Operational Resilience

The importance of businesses being 'operationally resilient' is becoming increasingly important, and a driving force behind whether an organization can ensure that its valuable business operations can 'bounce back' from or manage to evade impactful occurrences is its security risk management capabilities.

In this book, we change the perspective on an organization's operational resilience capabilities so that it changes from being a reactive (tick box) approach to being proactive. The perspectives of every chapter in this book focus on risk profiles and how your business can reduce these profiles using effective mitigation measures.

The book is divided into two sections:

1. Security Risk Management (SRM).
   All the components of security risk management contribute to your organization's operational resilience capabilities, to help reduce your risks.
   - Reduce the probability/likelihood.
2. Survive to Operate.
   If your SRM capabilities fail your organization, these are the components that are needed to allow you to quickly 'bounce back.'
   - Reduce the severity/impact.

Rather than looking at this from an operational resilience compliance capabilities aspect, we have written these to be agnostic of any specific operational resilience framework (e.g., CERT RMM, ISO 22316, SP 800-160 Vol. 2 Rev. 1, etc.), with the idea of looking at operational resilience through a risk management lens instead.

This book is not intended to replace these numerous operational resilience standards/frameworks but, rather, has been designed to complement them by getting you to appreciate their value in helping to identify and mitigate your operational resilience risks.

Unlike the cybersecurity or information security domains, operational resilience looks at the risks from a business-oriented view, so that anything that might disrupt your essential business operations are risk-assessed and appropriate countermeasures identified and applied.

Consequently, this book is not limited to cyberattacks or the loss of sensitive data but, instead, looks at things from a holistic business-based perspective.

First edition published 2024
by CRC Press
6000 Broken Sound Parkway NW, Suite 300, Boca Raton, FL 33487-2742

and by CRC Press
4 Park Square, Milton Park, Abingdon, Oxon, OX14 4RN

CRC Press is an imprint of Taylor & Francis Group, LLC

Library of Congress Cataloging-in-Publication Data
Names: Seaman, Jim (Writer on data protection), author. | Gioia, Michael, author.
Title: Security risk management : the driving force for operational resilience : the firefighting paradox / Jim Seaman and Michael Gioia.
Description: First edition. | Boca Raton : CRC Press, 2024. |
Series: Security, audit and leadership | Includes bibliographical references.
Identifiers: LCCN 2023004592 (print) | LCCN 2023004593 (ebook) |
ISBN 9781032263885 (hardback) | ISBN 9781032263892 (paperback) |
ISBN 9781003288084 (ebook)
Subjects: LCSH: Organizational resilience. | Business planning. |
Industries–Security measures. | Risk management. | Crisis management.
Classification: LCC HD58.9 .S436 2024 (print) | LCC HD58.9 (ebook) |
DDC 658.4/013–dc23/eng/20230614
LC record available at https://lccn.loc.gov/2023004592
LC ebook record available at https://lccn.loc.gov/2023004593

ISBN: 9781032263885 (hbk)
ISBN: 9781032263892 (pbk)
ISBN: 9781003288084 (ebk)

DOI: 10.1201/9781003288084

Typeset in Sabon
by Newgen Publishing UK

Contents

About the Authors

Jim Seaman honed his skills and craft during a 22-year career in the Royal Air Force Police, with the final decade being employed on counterintelligence, computer security, counterterrorism and risk management duties. On completion of his 22 years of military service, he sought the new challenge of transferring his specialist skills and knowledge across to the corporate sector. In the decade since transitioning across to the corporate environment, he has fulfilled roles within Payment Card Industry Data Security Standard (PCI DSS) compliance, data protection, information security, industrial systems security, and risk management. In the past few years, he has sought to further develop his knowledge and to rise to the challenge of authoring two books, one on the subject of PCI DSS (published May 2020) and the other on protective security (published April 2021).

Michael Gioia is an information security leader with over 18 years' experience of delivering security solutions across several industries. He has served as an officer in the United States Air Force and worked in higher education, the Department of Defense, retail food services, and security consulting. He has performed most of his information security work within higher education, currently, as the Chief Information Security Officer for Babson College and formerly as the Information Security Officer at Eastern Illinois University, Rose-Hulman Institute of Technology, and Bentley University. He retains various professional certifications that include a Certified Information Security Manager and Certified Data Privacy Solutions Engineer from ISACA, Certified Information System Security Professional from ISC2, GIAC Security Leadership Certification from SANS, and Payment Card Industry Professional from the PCI Security Standards Council.

Introduction

All too frequently, businesses do not focus enough on the value that security risk management (SRM) can bring to the defense of their organization. Instead, they will all too often regard SRM as an afterthought and as something that should only be conducted after something has happened or something has gone wrong. The authors of this book will argue that the driving force for operational resilience should and must be leveraged, as the result of the proactive application of SRM practices.

Would you ever imagine teaching a child the safe way to navigate across a busy road, without them first risk-assessing the conditions?

Imagine what the situation would be like if parents and schoolteachers applied the same approach that many business leadership teams appear to have adopted:

- Before stepping out into the road, the child does not need to look for hazards (threats) or consider the weather conditions, or even worry about the speed or type of vehicles traveling along the road.

In its place, the child only needs to consider conducting a risk assessment after they have been hit by a speeding vehicle. As a result (if they live), they can understand the risks of what mistakes they made and the damage caused, to help them apply the lessons learned.

As presented in the analogy above, reactive–rather than proactive–risk assessment can be incredibly costly. The authors of this book will present the concept that SRM should be behind every decision made and every implemented security measure, so that the business leadership teams have a better understanding of why these (often expensive) measures are implemented, which valued business operations/assets they are helping to mitigate, and what the associated risks are.

In today's modern business operations, it seems common sense that the leadership teams would want to ensure that their valued operations remain robust and able to quickly bounce back from impactful occurrences.

DOI: 10.1201/9781003288084-1

However, this does not appear to be the case, meaning that some areas of the globe have seen a need to bring in legislation (e.g., DORA (*Regulation of the European Parliament and of the Council on Digital Operational Resilience for the Financial Sector and Amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014*[1]) so that some regulators (e.g., (Financial Conduct Authority (FCA), "FCA Handbook: SYSC 15A.2 Operational Resilience Requirements"[2]) have powers to enable them to 'encourage' the financial services sector to consider how they can maintain their operational resilience.

In addition to the FCA's guidance, under the topic of operational risk, the Basel Committee (Basel Committee on Banking Supervision[3]) and the Bank of England[4] have created a comprehensive guide on the subject of Operational Resilience. This is stringently enforced within the Saudi Arabian banking rules (Saudi Arabian Monetary Authority[5] and this area is starting to gather pace, Internationally, (Price Waterhouse Cooper (PWC)[6]).

The UK FCA's, "Operational Resilience"[7]) has defined operational resilience as being: "*The capability of firms, financial market infrastructures and the financial sector to prevent, adapt and respond to, recover and learn from operational disruption.*"

This book is delivered through two distinct sections:

1. Security Risk Management
   Some of the SRM considerations and the supporting mitigation measures that are needed to help forge operationally resilient business operations.
   - Reducing the probability/likelihood.
2. 'Survive to Operate'
   Let's face it, no business operation can ever truly be 100% operational and secure 100% of the time. People will make mistakes or let their guards down, and risk can never be fully eradicated.
   - Reducing the impacts/consequences.

Notes

1 Regulation of the European Parliament and of the Council on Digital Operational Resilience for the Financial Sector and Amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014. 24 Sept. 2020.

2 Financial Conduct Authority (FCA). "FCA Handbook: SYSC 15A.2 Operational Resilience Requirements." Financial Conduct Authority (FCA), 31 Mar. 2022, www.handbook.fca.org.uk/handbook/SYSC/15A/2.html?date=2022-03-31. Accessed 25 Aug. 2022.

3 Basel Committee on Banking Supervision. Principles for Operational Resilience. Bank for International Settlements, Mar. 2021.

4 Bank of England (BoE). "Operational Resilience." www.bankofengland.co.uk, Mar. 2021, www.bankofengland.co.uk/prudential-regulation/publication/2021/march/operational-resilience-sop. Accessed 26 Aug. 2022.
5 Saudi Arabian Monetary Authority. Cyber Security Framework Saudi Arabian Monetary Authority. 2017.
6 Price Waterhouse Cooper (PWC). "Comparing International Expectations on Operational Resilience." Apr. 2021.
7 UK Financial Conduct Authority. "Operational Resilience." 17 May 2017, www.fca.org.uk/firms/operational-resilience

Section One

Security Risk Management

Reducing the Likelihood/Probability

Chapter 1

Finagling Your Business

Think of this approach as being like snowflakes…

If you allow snowflakes to continue to fall, land and settle without being noticed, they get deeper and deeper with no risks being perceived and no protective measures being prepared.

Then something causes these large accumulations of snowflakes to be disturbed and before you know it…

Avalanche!!!!

1.1 THE FINAGLE ANALOGY

Imagine that you are the owner and the driver of a motor vehicle. The local laws require that this vehicle must remain road legal and safe. Annually, your vehicle must undergo a government safety test to obtain a certificate for its roadworthiness.

Now, when buying the vehicle, you did not consider how much it might cost to support the vehicle's roadworthiness. Consequently, when the annual road safety test comes around, you realize that the tires' tread depth does not meet the smallest expected standards to pass the annual road safety test.

However, you need the car to be operational. As a result, you decide to 'finagle' the annual roadworthiness test by borrowing the wheels (with road-legal tires) from your friend's identical car. Hey presto! You get through the annual roadworthiness evaluation and obtain the annual certificate. Afterwards, you change the wheels back so that your friend gets his wheels back. However, your motor vehicle now has its old threadbare tires back.

The short-term gain of having achieved the annual roadworthiness certificate does not negate the fact that your vehicle is unsafe and is likely to lose traction or will have its stopping distance, under braking, severely affected.

- Does this not sound like the actions of desperation?
- Can you understand the risks of such a strategy?

DOI: 10.1201/9781003288084-3

1.2 INTRODUCTION

Throughout our professional careers, we have been astounded by the attitudes of some of our peers and, more importantly, business leaders. Increasingly there are companies that look to adopt a similar approach to the analogy when running their own businesses. If you think of the business as being like a motor vehicle, it has many moving parts that interact and support each other. For the business to remain successful, these moving parts need to remain operational. This is what is needed for the business to remain operationally resilient.

Gartner[1] defines operational resilience:

> *As initiatives that expand business continuity management programs to focus on the impacts, connected risk appetite and tolerance levels for disruption of product or service delivery to internal and external stakeholders (such as employees, customers, citizens and partners).*
>
> *These initiatives coordinate management of risk assessments, risk monitoring and execution of controls that impact workforce, processes, facilities, technology (IT, OT, IoT, physical and cyber-physical) and third parties across the following risk domains used in the business delivery and value realization process:*
> - *Security (cyber and physical),*
> - *Safety,*
> - *Privacy,*
> - *Continuity of operations,*
> - *Reliability.*

The difference between running a motor vehicle and keeping an operationally resilient company is that in a corporate environment this may be extremely complex, with many moving parts and processes being involved, and the things 'that could go wrong' may be extremely varied and the threats may be considerable in both type and volume.

Just a single failure of a critical asset or process could have catastrophic implications for the business. Such issues can also be caused by a plethora of causes; for example, IT system outage, IT software failure, human error, cyberattack, natural disaster, malware, etc.

To address this issue, it is vital for business leadership to stop thinking in isolated terms, such as:

- Cybersecurity
  Looking into the origins of this term, the constructs are broken down in the Etymology Online Dictionary ("Cyber- | Search Online Etymology Dictionary"[2]), as follows:

Word-forming component, ultimately from cybernetics (q.v.). It became a 'buzz word' with the rise of the internet early 1990s. One researcher (Nagel) counted 104 words formed from it by 1994. Cyberpunk (by 1986) and cyberspace (1982) were among the earliest. The OED 2nd edition (1989) has only cybernetics and its related forms, and cybernation "theory, practice, or condition of control by machines" (1962).

Security, (Online Etymology Dictionary[3]):

Early 15c., securite, "state or condition of being safe from danger or harm;" mid-15c., "freedom from care or anxiety" (a sense now archaic), from Old French securite and directly from Latin securitas "freedom from care," from securus "free from care" (see secure (adj.)).

Cybersecurity (Merriam-Webster Dictionary[4]):

"Mitigation measures taken to help protect a computer or computer system (as on the Internet) against unauthorized access or attack."

Should you only be concerned about those company assets that are internet-facing?

- Information Security (The Free Dictionary (Information Security)[5])
  The protection of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users.

  Information security includes those measures necessary to detect, document, and counter such threats. Information security includes computer security and communications security.

- Network security (Cisco[6])
  "Network security is the protection of the underlying networking infrastructure from unauthorized access, misuse, or theft. It involves creating a secure infrastructure for devices, applications, users, and applications to work in a secure manner."

  What about those assets that have no connectivity to any network infrastructures?

- Physical Security (What Is Physical Security? – Definition from Techopedia[7])
  The measures designed to ensure the physical protection of IT assets like facilities, equipment, personnel, resources and other properties from damage and unauthorized physical access. Physical security

measures are taken to protect these assets from physical threats including theft, vandalism, fire and natural disasters.

All these security industry terms are measures that, when used in combination, can help an organization to increase its operational resilience and reduce its risks. Consequently, it is important for corporations to move away from using these isolated terms and to adopt a more holistic risk-focused approach, to identify what their potential risks are and how the construct of these terms can help the business to reduce these risks to within acceptable parameters.

The title of the book, this chapter, and the security operations chapters are the limited places that you will read the term 'security,' as the focus of the content is on helping the reader to appreciate the value of being more directly risk-focused to enhance your organization's ability to continue operating through adverse events, or to have the ability to quickly 'bounce back' from unexpected, impactful events or incidents.

1.3 THE IMPORTANCE OF EFFECTIVE SECURITY RISK MANAGEMENT

Rather than thinking in terms of security or compliance, if an organization can move to a risk-focused approach everything else tends to fall into place.

- **Compliance** (Compliance | Etymology, Origin and Meaning of Compliance by Etymonline[8]):
  "1640s, 'act of complying; disposition to yield to others,' from comply + -ance. Related: Compliancy."
- **Security** (Security | Search Online Etymology Dictionary[9]):
  "Mid-15c., 'condition of being secure,' from Latin *securitas*, from *securus* 'free from care' (see secure). Replacing *sikerte* (early 15c.), from an earlier borrowing from Latin; earlier in the sense 'security' was *sikerhede* (early 13c.); *sikernesse* (c. 1200)."
- **Assurance** (Assurance | Etymology, Origin and Meaning of Assurance by Etymonline[10]).
  "Late 14c., 'formal or solemn pledge, promise,' also 'certainty, full confidence,' from Old French *asseurance* 'assurance, promise; truce; certainty, safety, security' (11c., Modern French assurance), from *asseurer* 'to reassure, to render sure' (see assure). Meaning 'self-confident' is from 1590s."

In fact, by finding and mitigating the risks to your business operations, you are significantly closer to achieving your compliance or security objectives. For example, if your business is seeking to achieve ISO/IEC 27001 or PCI

DSS compliance, the focus is to find and apply suitable mitigation security controls to mitigate the risks to your business operations and/or assets.

In ISO/IEC 27001, this is based upon your defined scope for the valued business assets and/or operations that you want to protect. Whereas, in PCI DSS, the scope is defined for you, with this being against any asset involved in the processing, storage, or transmission of cardholder data (or anything that could affect, or is connected to, these assets), and the valued assets are those that support the cardholder data operations.

To truly appreciate the value of SRM and how it differs from security or compliance, you need to be able to recognize that security and compliance are reactive strategies, while when applied effectively SRM can be proactive. However, it is important to note that SRM is not an exact science but rather a means of forecasting that something 'might' happen and what the potential impact might be.

The objective of an effective SRM practice should be to articulate to the business a realistic risk scenario, so that the forecasted risks can be calculated, and the key stakeholders and/or risk owners can make an informed decision on, should the forecasted risk occur, whether the business is suitably prepared and whether they are comfortable with these risks or not.

The output of a risk assessment should lead the business to create and document a suitable risk response (National Institute of Standards and Technology (NIST)[11]), as detailed in Table 1.1.

The risk response stage follows the risk assessment and is a critical part of any SRM process, as detailed in the NIST Risk Management Framework (NIST, Risk Management Framework for Information Systems and Organizations[12]).

Table 1.1 Risk Response

Traditional	*5 T's*	*Description*
Accept	Tolerate	This consists in identifying the risks and documenting all the risk management information about it, but being comfortable that no action is required, unless the risk occurs.
Avoid	Terminate	Ending the threat by any means available.
Mitigate	Treat	Applying a proper level of risk treatment options that bring the risks to a level that the business risk owners are comfortable with.
Transfer	Transfer	Utilize a third party to take the responsibility for reducing the risk. However, you will still have accountability for ensuring that the third party continues to reduce the risk to within acceptable tolerances.
	Take the opportunity	Finding risk and, rather than resolving it, using this to gain a short-term advantage.

1. Prepare to execute the risk management framework (RMF) from an organization- and a system-level perspective by establishing a context and priorities for managing security and privacy risk.
2. Categorize the system and the information processed, stored, and transmitted by system, based on an analysis of the impact of loss.
3. Select an initial set of controls for the system and tailor the controls as needed to reduce risk to an acceptable level based on an assessment of risk.
4. Implement the controls and describe how the controls are employed within the system and its environment of operation.
5. Assess the controls to determine whether the controls are implemented correctly, operating as intended, and producing the desired outcomes with respect to satisfying the security and privacy requirements.
6. Authorize the system or common controls based on a determination that the risk to organizational operations and assets, individuals, other organizations, and the nation is acceptable.
7. Monitor the system and the associated controls on an ongoing basis to include assessing control effectiveness, documenting changes to the system and environment of operation, conducting risk assessments and impact analyses, and reporting the security and privacy posture of the system.

1.4 TO FINAGLE OR NOT TO FINAGLE? THAT IS THE QUESTION

If I had a £1 or $1 for each time that I heard a business key stakeholder or subject matter expert (SME) suggest the advantages of avoiding doing something to save themselves time, effort, or investment, I would be an extremely rich man.

It had been exceedingly difficult to understand and appreciate why these people would suggest such a thing if the thing they were suggesting would be potentially detrimental to the business or would significantly increase the risks for the organization.

That was until I had dealings with an individual who was in a very senior position within a highly respected IT services company and whose role was to supply specialist governance, risk, and compliance support to the organization's key stakeholders and to supply assurances to their many customers.

While working with this individual (to help prepare the business for an annual 'roadworthiness' check), during a pre-check discussion with one of the SMEs, the SME stated that a mitigation measure was not in place and, as far as they knew, had never been in place. Subsequently, they asked how the company had managed to pass previous 'roadworthiness' assessments.

This individual's response blew my mind: "We finagled it!"

He used a term that I had never heard before and was one that I had to look up in the dictionary ("Definition of Finagle | Dictionary.com"[13]): "To trick, swindle, or cheat (a person) (often followed by out of): He finagled the backers out of a fortune."

Of course, this should not be confused with the term 'Finagle's Law' (Bureman)[14]: "In its most general form, is the idea that anything that can go wrong will go wrong, and usually in the most disastrous way imaginable."

No doubt you have had days when you have felt as if you have been subject to Finagle's Law. However, in an organization that supports the finagling of the business, rather than adopting a risk-focused and balanced approach, Finagle's Law can often become a common part of daily business operations, which, of course, it should never be!

How often have you heard a security SME use the sentence, "It feels like all I do is fight fires!"?

1.5 THE FIREFIGHTING PARADOX

No matter the size or type of your business, no doubt you will face periods when you feel as if you are constantly fighting fires in response to the company's demands. At the same time, you are expected to manage the risks and keep all critical systems and operations safe, while defending against opportunist attackers, as well as protecting the business from the insider risk (deliberate or accidental actions of employees that present a danger to the business).

The 'firefighting' paradox is a term that is well known beyond the security industry and extends well into the business environment. The problem with having a 'firefighting' approach is that, without incorporating a risk management strategy to it, the business has a limited knowledge of which fires need to be prioritized and, as a result, the more impactful fires can be neglected by individuals that are responding to those fires that are more visible to the business. Consequently, the less visible fires that are associated with the more critical parts of the business remain unquenched, leading to significantly more impact and damage to the business.

In the July–August 2000 *Harvard Business Review* magazine, there was a useful article that described the need to 'Stop Fighting Fires,' (Bohn[15]). In this article, the author explains what the term means but then goes on to describe a simple model of firefighting in which the author supplies a depiction of something that most of us will have experienced at first hand: How problems flow through an organization, as depicted in Figure 1.1.

I would be incredibly surprised if no one reading this book has experienced those occasions when you might be expected to tear yourself into several pieces, so that you can solve everyone's problems that are clearly the most important and should be prioritized over anyone else's.

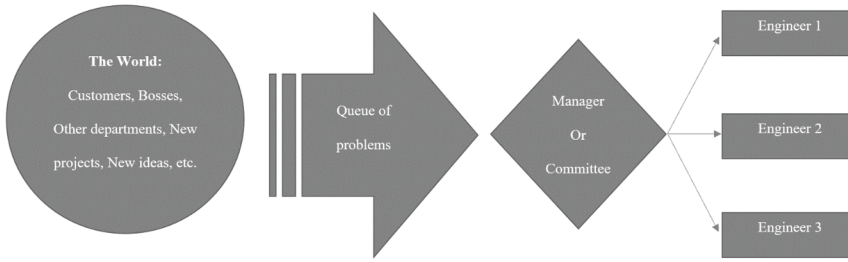


Figure 1.1 Organization problem flows.

$$\textbf{Traffic intensity} = \frac{\text{(Days to solve) X (Number of new problems per day)}}{\text{Number of engineers}}$$

Figure 1.2 Traffic intensity equation.

This article then tries to explain the value of understanding the traffic intensity, so that a better appreciation can be formulated, based upon the number of days needed to resolve the problem, the number of the latest problems per day and the amount of resources, as depicted in their equation in Figure 1.2.

Without a clear understanding of the potential traffic intensity, it is unlikely that your business will ever stop employing firefighting strategies, which can become increasingly detrimental to your business and can lead to a pressure cooker of working conditions. This, in turn, could result in increased stress to the business teams, which leads to higher sickness or levels of staff turnover.

All of this increases the insider threat, where employees can become disillusioned with the company or, due to increased pressures and workloads, have an increased likelihood of taking shortcuts or making mistakes.

The NIST[16] defines insider risk as being:

> The threat that an insider will use her/his authorized access, wittingly or unwittingly, to do harm to the security of organizational operations and assets, individuals, other organizations, and the Nation. This threat can include damage through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of organizational resources or capabilities.

In risk-managing operational resilience capabilities, a 'firefighting' approach can prove to be extremely detrimental, as while you are constantly jumping from one fire to another, you are given limited time to take stock and reflect

on what went well, and what areas could be improved (lessons learned). As a result, you increase the risks of an impactful incident reoccurring and potentially being more harmful to the company if a more critical asset or process is affected on the repeat occasion.

In addition, you do not have the time to investigate any emerging threats so that you can adapt your defensive strategy, so that it still is current and effective.

By having a risk-focused approach to your operational resilience strategies, you will be better able to triage your responses. This is especially relevant to those businesses that use a 'lean' business model, ("What Is a Lean Business Model? – Definition | Meaning | Example"[17]): "How do you run an effective operationally resilient business, using the Lean Business Model, if you don't understand the risks or what resources are needing to keep the business roadworthy, safe and operational?"

1.6 THE PSYCHOLOGY OF FINAGLING

Knowing how detrimental finagling can be to a business, why is it that so many business leaders and information security SMEs lean toward a finagled approach to reporting the 'State of the Nation'?

This all comes down to human psychology and an individual's natural leaning to employ their ego defense mechanisms. In the 1890s, Sigmund Freud found that human beings had ten ego defense mechanisms that they unconsciously use to protect themselves from anxiety rising through undesirable thoughts or feelings. These ten defense mechanisms consist of the following, (Mcleod[18]), as depicted in Table 1.2.

Often it is said that security requires a 'top-down' approach so that we obtain senior management, or C-Level ("Definition of C-Level | Dictionary.com"[19]) executive buy-in and support. However, what if the C-Level or the person responsible for communicating the risks to the C-Level are unconsciously employing these defensive mechanisms?

Within an organization it is extremely likely that you are going to have several of the nine Belbin team roles, and each can be complementary to each other to create an effective business culture (Team Roles and Organisational Culture[20]), when they are evenly dispersed across an organization. Belbin named nine individual team roles, as depicted in Table 1.3 (Belbin[21]).

As you can imagine, each of these team roles naturally lends itself to the individuals adopting one or more of these defensive mechanisms to help them survive and be successful in their professional career. As a result, you may find that these individuals and their defensive mechanisms have opposite effects on the way that risks are communicated and mitigated against.

For example, let's take a situation where a C-Suite member is a natural 'implementer.' Such an individual is known as action-oriented, with a tendency to lack flexibility and to be very rigid in their approach. Now, if your

Table 1.2 Ten Defense Mechanisms

1. Denial	An individual does not report or accept any reports that there are any issues, problems, or concerns. By not accepting the facts, they are trying to absolve themselves of the consequences or the potential impact on the organization. *Ignore it and hope it will go away or not happen.*
2. Repression	This is when an individual experiences or think things may be threatening but may choose to repress them instead of dealing with the issue or problem. *Bury your head in the sand.*
3. Projection	Rather than acknowledging threatening traits in themselves, the individual points these same traits out in others instead. *Displacing personal feelings onto others.*
4. Displacement	Displacement is the redirection of an impulse (usually aggression) onto a powerless substitute target. *The blame game.*
5. Regression	This is where an individual reverts to display age-inappropriate behavior and adopt immature traits and emotions. *Acting like a child.*
6. Sublimation	This is like displacement; however, this takes place when an individual manages to displace their unacceptable emotions into constructive and socially acceptable behaviors. *Channeling emotions.*
7. Rationalization	This a cognitive distortion of 'the facts' to make an event or an impulse less threatening. *Lying to oneself.*
8. Reaction Formation	This is when an individual goes beyond denial and acts in a manner that is the opposite to the way they think or feel. *Faking it.*
9. Introjection	This is when an individual adopts the personality characteristics of another, to help solve an emotional difficulty. *Mirroring.*
10. Identification with the Aggressor	This is where an individual adopts the behavior of someone who is more powerful and hostile toward them. *Becoming the bully.*

information security manager happens to be a 'teamworker,' rather than being a good thing for the business this could turn out to be the complete opposite. The 'teamworker' is known for being people-oriented and may be very sensitive and avoid hard decisions. As a result, they tend to have calm temperaments and are often extremely diplomatic in their approach.

This combination of natural team roles and their adopted defensive mechanisms can become extremely obstructive, with any significant risks either not being reported or the risk reports falling on deaf ears.

Imagine if the C-Suite member ('implementer') has adopted the denial defense mechanism and the information security manager (teamworker) has adopted the rationalization defense mechanism:

Table 1.3 Belbin Team Roles

Team Role	*Description*
Resource Investigator	Uses their inquisitive nature to find ideas to bring back to the team. Strengths: Outgoing, enthusiastic. Explores opportunities and develops contacts. Allowable weaknesses: Might be over-optimistic and can lose interest once the initial enthusiasm has passed. Do not be surprised to find that: They might forget to follow up on a lead.
Teamworker	Helps the team to gel, using their versatility to identify the work required and complete it on behalf of the team. Strengths: Cooperative, perceptive, and diplomatic. Listens and averts friction. Allowable weaknesses: Can be indecisive in crunch situations and tends to avoid confrontation. Do not be surprised to find that: They might be hesitant to make unpopular decisions.
Coordinator	Needed to focus on the team's objectives, draw out team members, and delegate work appropriately. Strengths: Mature, confident, identifies talent. Clarifies goals. Allowable weaknesses: Can be seen as manipulative and might offload their own share of the work. Do not be surprised to find that: They might over-delegate, leaving themselves little work to do.
Plant	Tends to be highly creative and good at solving problems in unconventional ways. Strengths: Creative, imaginative, free-thinking, generates ideas, and solves difficult problems. Allowable weaknesses: Might ignore incidentals and may be too preoccupied to communicate effectively. Do not be surprised to find that: They could be absent-minded or forgetful.
Monitor Evaluator	Provides a logical eye, making impartial judgments where required and weighs up the team's options in a dispassionate way. Strengths: Sober, strategic, and discerning. Sees all options and judges accurately. Allowable weaknesses: Sometimes lacks the drive and ability to inspire others and can be overly critical. Do not be surprised to find that: They could be slow to come to decisions.
Specialist	Brings in-depth knowledge of a key area to the team. Strengths: Single-minded, self-starting, and dedicated. They provide specialist knowledge and skills. Allowable weaknesses: Tends to contribute on a narrow front and can dwell on the technicalities. Do not be surprised to find that: They overload you with information.

(*Continued*)

Table 1.3 (Continued)

Team Role	*Description*
Shaper	Provides the necessary drive to ensure that the team keeps moving and does not lose focus or momentum. Strengths: Challenging, dynamic, thrives on pressure. Has the drive and courage to overcome obstacles. Allowable weaknesses: Can be prone to provocation and may sometimes offend people's feelings. Do not be surprised to find that: They could risk becoming aggressive and bad-humored in their attempts to get things done.
Implementer	Needed to plan a workable strategy and carry it out as efficiently as possible. Strengths: Practical, reliable, efficient. Turns ideas into actions and organizes work that needs to be done. Allowable weaknesses: Can be a bit inflexible and slow to respond to new possibilities. Do not be surprised to find that: They might be slow to relinquish their plans in favor of positive changes.
Completer Finisher	Most effectively used at the end of tasks to polish and scrutinize the work for errors, subjecting it to the highest standards of quality control. Strengths: Painstaking, conscientious, anxious. Searches out errors. Polishes and perfects. Allowable weaknesses: Can be inclined to worry unduly, and reluctant to delegate. Do not be surprised to find that: They could be accused of taking their perfectionism to extremes.

- **Denial**: "Adopting a mode of defense which consists of the subject's refusing to recognize the reality of a traumatic perception." (Laplanche and Pontalis[22]).
- **Rationalization:** "Occurs when a person has performed an action and then concocts the beliefs and desires that would have made it rational. Then, people often adjust their own beliefs and desires to match the concocted ones." (Brody and Costa[23]).

The information security manager, being the natural diplomat, will lend themself to make life easier by only presenting positive spin/news to the C-Suite implementer. Therefore, the business becomes complacent, believing that it is facing few or no risks.

With a great deal of luck, this does not present any issues to the business leaders, who continue oblivious to the dangers that they might face, and any potential exploitable vulnerabilities remain untracked and are not risk-prioritized for remediation. However, the reality in an ever-increasing digital and internet-connected world, where the risks of a cyberattacks

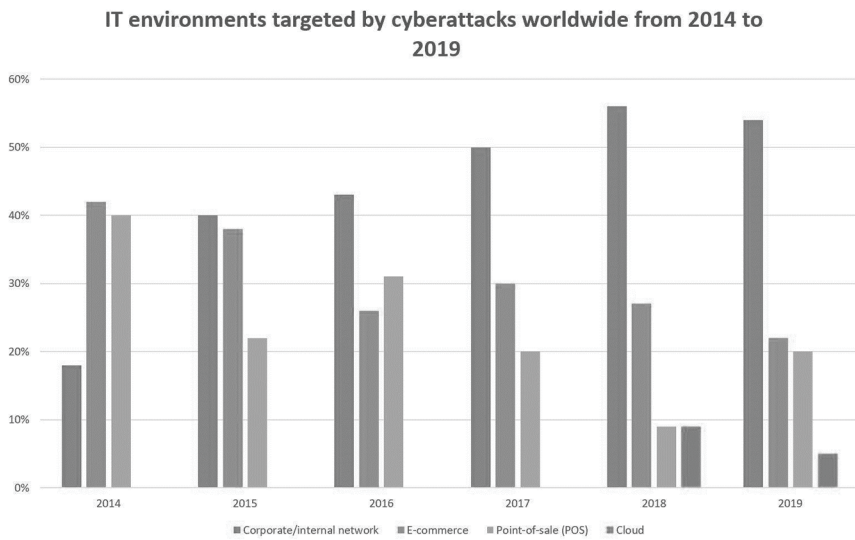


Figure 1.3 Cyberattack trends, 2014 to 2019.

grow exponentially, as shown in Figure 1.3 ("Cyber Attacks: Targeted IT Environments 2019"[24]) and Figure 1.4 ("Successful Cyber Attacks Launched Against Global Businesses 2021"[25]), relying on luck to safeguard your business becomes a very dangerous strategy.

1.7 EFFECTIVE RISK COMMUNICATION

Given individual character traits and their subconscious adoption of defensive mechanisms, as well as business pressures and the lack of technical knowledge, this can make the communication of risk extremely difficult to achieve. As a result, this might be an area where the risk reports are 'finagled,' and the produced risk reports may not be achieving the desired effects to help the business reduce prioritized risks, and you may only be going through the motions to tick an expected box.

- Are your risk reports being reviewed?
- Does the receiving audience ever ask questions on the content?
- Do the reports help to drive business decision-making decisions?

Cybersecurity/information security SMEs tend to want to prove how knowledgeable they are (worth their salaries), so they adopt the practice of making their risk messages too long and complex. As a result, the receiving audience does not understand the risks.

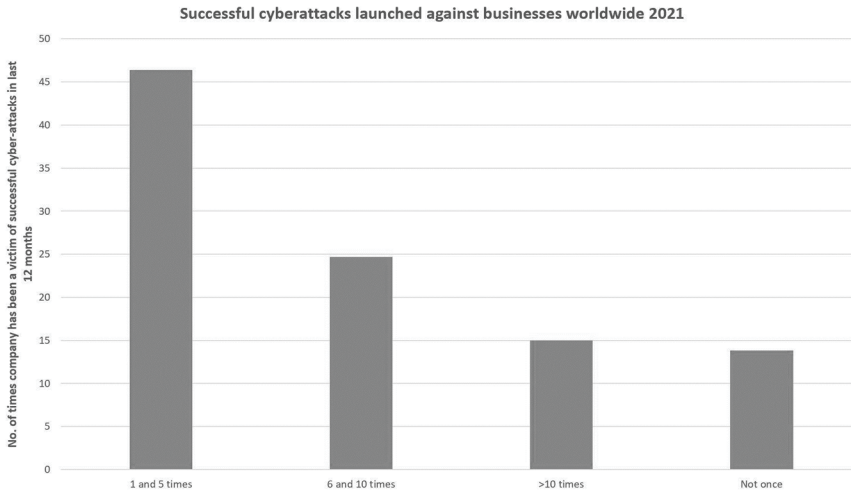


Figure 1.4 2021 successful cyberattacks.

Another factor to consider is whether you have prioritized the reported risks. You need to avoid sounding like 'Chicken Little,' ("The Story of Chicken Little: The Sky Is Falling"[26]) and sending out messages that articulate that the business world is falling in.

Another problem is that the receiving audience members got to where they are because they are proficient in their role responsibilities and not because they understand technology or threat profiles. Consequently, the risk messages need to be simplified so that they answer the 'so what?' question, and that the audience clearly understands the urgency and potential impacts that the risks present.

It is also important to remember that the receiving audience is extremely busy and has limited time availability. Consequently, it is extremely important to develop risk reports that easily convey the risk messages, in a clear easy-to-read format. Remember that a picture paints a thousand words, so consider the benefits of using graphs. You can gain exceptional value by periodically asking the receiving audience for some feedback on your risk reports.

- Do they find the risk reports easy to read and understand?
- Do the risk reports supply the information they need to make informed risk decisions?
- What improvements can be made to the risk reports?

1.8 WHEN SECURITY RISK MANAGEMENT BITES BACK

When a business does not focus on risk and, instead, focuses on 'ticking a box' for compliance or security assurance needs, they are faced with an increasing number of plates that need to be kept spinning and, ultimately, they can pay the price of focusing on keeping the wrong plate spinning, while a far more valuable plate falls to the ground and breaks.

For instance, look at British Airways (BA) and Claire's Accessories. Both being high-volume e-commerce merchants, they would have needed to have been annually assessed as being PCI DSS compliant. In fact, BA took security assurance and PCI DSS compliance so seriously that they even paid the PCI Security Standards Council (PCI SSC) a fee to be a 'participating organization,' as seen in the captured image on Wayback Machine for 21:23:06, on 14th September 2017, as depicted in Figure 1.5, ("Official PCI Security Standards Council Site – Verify PCI Compliance, Download Data Security and Credit Card Security Standards"[27]).

Over one year previously (6th October 2016) RiskIQ was reporting that e-commerce websites were victims of malicious script injections, (Spruell[28]). These types of attacks would serve as a man-in-the middle (MITM) style of attack, enabling the attacker to redirect the customers' payment journeys so that the customers went from the merchant's website, through the attacker's clandestine infrastructure, to the PCI DSS-compliant payment service provider (PSP)'s interface. As a result, when the customer typed their cardholder details into the PSP's interface, the attackers were able to electronically skim the customers' cardholder details.

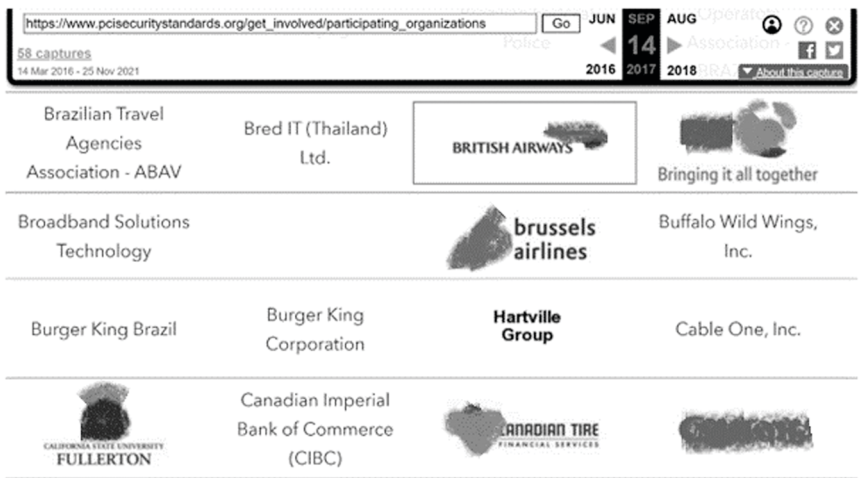


Figure 1.5 Wayback machine screen capture.

Despite this increased risk to e-commerce merchants, few risk-assessed their payment processes and, before long, despite the fact that BA had transferred the risk from payment process, through the use of a redirect or iFrame to a PCI DSS-compliant PSP, between 22:58 BST, 21st August 2018 until 21:45 BST, 5th September 2018 they were the victims of a Magecart group ("All You Need to Know about Magecart Hacking Groups"[29]) cyberattack, ("How Did Hackers Get into British Airways?"[30]). During this time, the Magecart Group 6, (Klijnsma[31]), managed to skim around 500,000 customer credit cards.

Magecart Group 6

Modus operandi
Group 6 was first observed using web-skimmers in 2018 but has a long history in the underground. Group 6 is perhaps the most high-profile Magecart group, and its impact has been huge. The group's approach is to be selective, only going for top-tier targets such as British Airways and Newegg, so that even if they only manage to hold the skimmer in place for a short period, the sheer volume of transactions on the victim website will yield a high return on investment.

The skimmer
Group 6's skimmer is very simple compared to those of the other groups. While the concept is the same as other Magecart skimmers, Group 6 operatives have a good knowledge of how their victim processes payments, which allows them to integrate their skimmer in a much more elegant – and less detectable – way.

Had BA been more risk-focused (proactive) and less motivated by compliance and security assurance, it would have identified that, despite its e-commerce website being PCI DSS compliant (reactive) against the shortened PCI SSC's SAQ A[32] security controls, it was still at risk from this type of MITM-style attack. This would have then enabled BA to apply added mitigation controls to help reduce this risk yet further.

There follows an extract from the earlier October 2018 version of the SAQ A ("Wayback Machine"[33]):

Payment Card Industry (PCI) Data Security Standard
Self-Assessment Questionnaire A and Attestation of Compliance
Card-not-present Merchants, All Cardholder Data Functions Fully Outsourced
For use with PCI DSS Version 3.2.1, June 2018

Before You Begin
SAQ A has been developed to address requirements applicable to merchants whose cardholder data functions are completely outsourced

to validated third parties, where the merchant retains only paper reports or receipts with cardholder data.

SAQ A merchants may be either e-commerce or mail/telephone-order merchants (card-not-present), and do not store, process, or transmit any cardholder data in electronic format on their systems or premises.

SAQ A merchants confirm that, for this payment channel:

- Your company accepts only card-not-present (e-commerce or mail/telephone-order) transactions.
- All processing of cardholder data is entirely outsourced to PCI DSS validated third-party service providers.
- Your company does not electronically store, process, or transmit any cardholder data on your systems or premises, but relies entirely on a third party(s) to handle all these functions.
- Your company has confirmed that all third-party(s) handling storage, processing, and/or transmission of cardholder data are PCI DSS compliant; and
- Any cardholder data your company retains is on paper (for example, printed reports or receipts), and these documents are not received electronically.

Additionally, for e-commerce channels:

- All elements of the payment page(s) delivered to the consumer's browser originate only and directly from a PCI DSS validated third-party service provider(s).

This SAQ is not applicable to face-to-face channels.

This shortened version of the SAQ includes questions that apply to a specific type of small merchant environment, as defined in the above eligibility criteria. If there are PCI DSS requirements applicable to your environment that are not covered in this SAQ, it may be an indication that this SAQ is not suitable for your environment. Additionally, you must still comply with all applicable PCI DSS requirements in order to be PCI DSS compliant.

Note: For this SAQ, PCI DSS Requirements that address the protection of computer systems (for example, Requirements 2, 6, and 8) apply to e-commerce merchants that redirect customers from their website to a third party for payment processing, and specifically to the merchant web server upon which the redirection mechanism is located. Mail order/telephone order (MOTO) or e-commerce merchants that have completely outsourced all operations (where there is no redirection mechanism from the merchant to the third party) and therefore do not have any systems in scope for this SAQ, would consider these

> requirements to be "not applicable." Refer to guidance on the following pages for how to report requirements that are not applicable.

Unfortunately, for BA and any e-commerce retailer, such as NewEgg (Lukic[34]), TicketMaster (Dunn[35]), Claire's Accessories (Scroxton[36]), etc. that employs an embedded iFrame or a redirect to a PCI DSS-compliant PSP to qualify for PCI DSS against the shortened SAQ, this leaves them wide open to a Magecart MITM-style attack. The shortened SAQ did not include essential security controls, such as:

> 6.1 Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as "high," "medium," or "low") to newly discovered security vulnerabilities.
>
> 12.2 Implement a risk-assessment process that:
>
> - Is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.),
> - Identifies critical assets, threats, and vulnerabilities, and
> - Results in a formal, documented analysis of risk.

With a focus on compliance and not on the risks to their e-commerce business operations, they were not required to keep track of any new vulnerabilities or to carry out risk assessments. As a result, the threat from the Magecart group cyberattacks went unnoticed, so no additional mitigation controls were applied to help protect their e-commerce operations from this new threat.

This clearly shows that, at the time, the card brands (Visa, Mastercard, Amex, JCB and Discovery) and the PCI SSC were comfortable with the convenience and the reduction of scope and effort that transferring the risk to a PCI DSS-compliant PSP provided. It was this convenience and lack of SRM that allowed the opportunist criminals to exploit this online payment journey.

1.9 THE SECURITY RISK MANAGEMENT ENABLER

Both information and IT systems have become the life support (e.g., Information Systems = Blood; Information/IT Systems = Vital organs; Intrusion Detection Systems = Nerve System, etc.) for most businesses and, as a result, it is important for organizations to remain vigilant to potential hazards and to have first aid and contingency plans to ensure that these systems remain healthy and operational. However, frequently, business risk and security practices are addressed in isolation rather than as being complementary to one another, much like an industrial or manufacturing

business might do with health and safety (H&S) (Health & Safety Authority, "Hazards and Risk"[37]):

> **What is a Hazard?**
> When we refer to hazards in relation to occupational safety and health the most commonly used definition is "A Hazard is a potential source of harm or adverse health effect on a person or people."
>
> The terms Hazard and Risk are often used interchangeably but this simple example explains the difference between the two.
>
> If there was a spill of water in a room then that water would present a slipping hazard to persons passing through it. If access to that area was prevented by a physical barrier, then the hazard would remain though the risk would be minimized.
>
> **What is Risk?**
> When we refer to risk in relation to occupational safety and health the most commonly used definition is "Risk is the likelihood that a person may be harmed or suffers adverse health effects if exposed to a hazard."

In such an organization, the business proactively encourages all its employees to report hazards. These hazards are then risk-assessed and prioritized for remediation, as part of the company's risk management practices. This should be the same for SRM, which should focus on the following:

1. What are the valuable assets of the business?
2. What vulnerabilities have been identified to these valued assets?
   - What are the vulnerability risk ratings?
3. What threat actors are likely to exploit these identified vulnerabilities?
4. What is the forecasted impact if these threat actors exploit the identified vulnerabilities?
5. Is the business comfortable with these risks?
   - Have you documented these risks and obtained the risk owners sign off?
   - What additional control measures are available to help treat any identified risk?

1.10 DECODING SECURITY RISK MANAGEMENT

Unfortunately, the value of security and compliance to an organization can be reduced by a lack of risk-focused practices. As a result, security- and compliance-driven approaches become reactive practices, with a lack of teamwork and visible return on investments.

Consequently, unlike H&S practices, a 'bare acceptable minimum' approach is adopted, whereby the business either becomes increasingly

comfortable with the hazards that it may face or is unaware of the risks that it faces and the potential impact that might occur as a result.

- Can you imagine a construction company director not investing in safety helmets for their construction workers, or a police officer not being issued body protection?

Much like the terms hazard and risk are interchangeable, the control measures are implemented/applied to help mitigate these hazards or risks. However, often, in the business environment the risk assessment for the company's life support systems are not given the same importance, and rather than applying proper defensive measures to any identified hazards or risks, these impactful risks are often not identified or risk-assessed, so are left untreated.

These untreated risks can present an opportunity for exploitation, which can lead to a compromise of the business's life support systems. This can then affect the health of the business operations or lead to a data breach (severed artery).

Much like H&S, SRM does not show a tangible return on investment; however, employers that invest in SRM can expect to reduce their risks from accidental or deliberate actions that result in a breach of data confidentiality, integrity, or availability, or IT system integrity or availability (outages). This will result in benefits in a variety of areas, such as reduced regulatory penalties, increased company reputation, and customer confidence. In addition, employers often find that changes made to improve SRM can result in significant improvements to their organization's productivity and financial performance, while creating a cohesive enterprise-wide risk culture.

In fact, in Gartner's Top 8 Cybersecurity Predictions for 2021–2022, it is forecasting that threat actors will be cause physical harm (Gartner, Panetta[38]), meaning that SRM could soon become more akin to H&S:

> 8. By 2025, threat actors will have weaponized operational technology environments successfully enough to cause human casualties.
>
> As malware spreads from IT to OT, it shifts the conversation from business disruption to physical harm with liability likely ending with the CEO. Focus on asset-centric cyber-physical systems, and make sure there are teams in place to address proper management.

Notes

1 Gartner. "Operational Resilience." 2012. www.gartner.com/en/information-technology/glossary/operational-resilience

2 "Cyber- | Search Online Etymology Dictionary." www.etymonline.com, www.etymonline.com/search?q=cyber-&ref=searchbar_searchhint. Accessed 7 Jan. 2022.

3 Online Etymology Dictionary. "Security | Origin and Meaning of Security by Online Etymology Dictionary." www.etymonline.com, 2022, www.etymonline.com/word/security#etymonline_v_30368. Accessed 23 July 2022.
4 Merriam-Webster Dictionary. "Definition of CYBERSECURITY." Merriam-Webster.com, 2019, www.merriam-webster.com/dictionary/cybersecurity. Accessed 23 July 2022.
5 "Information Security." TheFreeDictionary.com, www.thefreedictionary.com/information+security.
6 Cisco. "What Is Network Security?" Cisco, 2019, www.cisco.com/c/en/us/products/security/what-is-network-security.html
7 "What Is Physical Security? – Definition from Techopedia." Techopedia.com, 2020, www.techopedia.com/definition/14514/physical-security
8 "Compliance | Etymology, Origin and Meaning of Compliance by Etymonline." www.etymonline.com, www.etymonline.com/word/compliance#etymonline_v_28480. Accessed 7 Jan. 2022.
9 "Security | Search Online Etymology Dictionary." www.etymonline.com, www.etymonline.com/search?q=security
10 "Assurance | Etymology, Origin and Meaning of Assurance by Etymonline." www.etymonline.com, www.etymonline.com/word/assurance#etymonline_v_26630. Accessed 7 Jan. 2022.
11 NIST, CSRC Content. "Risk Response – Glossary | CSRC." Csrc.nist.gov, csrc.nist.gov/glossary/term/risk_response. Accessed 7 Jan. 2022.
12 NIST. Risk Management Framework for Information Systems and Organizations: Dec. 2018, nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf, 10.6028/nist.sp.800-37r2
13 "Definition of Finagle | Dictionary.com." www.dictionary.com, www.dictionary.com/browse/finagle. Accessed 7 Jan. 2022.
14 Bureman, Liz. "Finagle's Law: A Writer's Guide." The Write Practice, 26 Aug. 2014, thewritepractice.com/finagles-law. Accessed 7 Jan. 2022.
15 Bohn, Roger. "Stop Fighting Fires." *Harvard Business Review*, 1 July 2000, hbr.org/2000/07/stop-fighting-fires
16 NIST. "Security and Privacy Controls for Information Systems and Organizations." *Security and Privacy Controls for Information Systems and Organizations*, 5 (23), Sept. 2020, nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf, 10.6028/nist.sp.800-53r5. Accessed 22 Aug. 2022.
17 "What Is a Lean Business Model? – Definition | Meaning | Example." My Accounting Course, 2019, www.myaccountingcourse.com/accounting-dictionary/lean-business-model
18 Mcleod, Saul. "Defense Mechanisms." Simplypsychology.org, *Simply Psychology*, 10 Apr. 2019, www.simplypsychology.org/defense-mechanisms.html
19 "Definition of C-Level | Dictionary.com." www.dictionary.com/browse/c-level. Accessed 7 Jan. 2022.
20 "Team Roles and Organisational Culture." www.belbin.com/resources/blogs/team-roles-and-culture. Accessed 7 Jan. 2022.
21 Belbin. "Belbin Team Roles." Belbin.com, Belbin, www.belbin.com/about/belbin-team-roles.
22 Laplanche, Jean, and Pontalis, Jean-Bertrand. The Language of Psycho-Analysis. London, The Hogarth Press, 1973.

23 Brody, Stuart, and Costa, Rui. (2020). Rationalization is a suboptimal defense mechanism associated with clinical and forensic problems. *Behavioral and Brain Sciences*, 43.
24 "Cyber Attacks: Targeted IT Environments 2019." Statista, www.statista.com/statistics/434764/it-environment-cyber-crime-attack
25 "Successful Cyber Attacks Launched Against Global Businesses 2021." Statista, www.statista.com/statistics/221394/successful-cyber-attacks-launched-against-businesses-worldwide. Accessed 7 Jan. 2022.
26 "The Story of Chicken Little: The Sky Is Falling." www.dltk-Teach.com, www.dltk-teach.com/fairy-tales/chicken-little/story.htm
27 "Official PCI Security Standards Council Site – Verify PCI Compliance, Download Data Security and Credit Card Security Standards." web.archive.org, 14 Sept. 2017, web.archive.org/web/20170914212306/www.pcisecuritystandards.org/get_involved/participating_organizations. Accessed 7 Jan. 2022.
28 Spruell, Darren. "Compromised E-Commerce Sites Lead to 'Magecart'" | RiskIQ. 6 Oct. 2016, www.riskiq.com/blog/labs/magecart-keylogger-injection. Accessed 7 Jan. 2022.
29 "All You Need to Know about Magecart Hacking Groups." Reflectiz, 4 May 2021, www.reflectiz.com/blog/magecart-hacking-groups-how-they-are-expanding-their-limits-beyond-the-regular-e-commerce-websites. Accessed 7 Jan. 2022.
30 "How Did Hackers Get into British Airways?" BBC News, 7 Sept. 2018, www.bbc.co.uk/news/technology-45446529
31 Klijnsma, Yonathan. "Virus Bulletin: VB2019 Paper: Inside Magecart: The History Behind the Covert Card-Skimming Assault on the E-Commerce Industry." www.virusbulletin.com, 2019, www.virusbulletin.com/virusbulletin/2019/10/vb2019-paper-inside-magecart-history-behind-covert-card-skimming-assault-e-commerce-industry. Accessed 7 Jan. 2022.
32 Payment Card Industry (PCI) Data Security Standard Self-Assessment Questionnaire A and Attestation of Compliance Card-Not-Present Merchants, All Cardholder Data Functions Fully Outsourced for Use with PCI DSS Version 3.2.1. 2018.
33 "Wayback Machine." web.archive.org. www.pcisecuritystandards.org/documents/PCI-DSS-v3_2_1-SAQ-A.pdf. Accessed 7 Jan. 2022.
34 Lukic, David. "Is Newegg Safe? The Story of Newegg Hack." IDStrong, 20 Oct. 2020, www.idstrong.com/sentinel/the-newegg-data-breach. Accessed 7 Jan. 2022.
35 Dunn, John. "The Ticketmaster Breach – What Happened and What to Do." Naked Security, 28 June 2018, nakedsecurity.sophos.com/2018/06/28/ticketmaster-breach-what-happened-and-what-to-do. Accessed 7 Jan. 2022.
36 Scroxton, Alex. "Accessories Store Claire's Hit by Magecart Credit Card Fraudsters." ComputerWeekly.com, 15 June 2020, www.computerweekly.com/news/252484652/Accessories-store-Claires-hit-by-Magecart-credit-card-fraudsters
37 "Hazards and Risk." Health and Safety Authority, www.hsa.ie/eng/Topics/Hazards
38 Panetta, Kasey. "The Top 8 Cybersecurity Predictions for 2021–2022." Gartner, 21 Oct. 2021, www.gartner.com/en/articles/the-top-8-cybersecurity-predictions-for-2021-2022

SECURITY, AUDIT AND LEADERSHIP SERIES

PRIVACY IN PRACTICE

Establish and Operationalize a Holistic Data Privacy Program

Alan Tang

CRC Press
Taylor & Francis Group

Privacy in Practice

Privacy is not just the right to be left alone, but also the right to autonomy, control, and access to your personal data. The employment of new technologies over the last three decades drives personal data to play an increasingly important role in our economies, societies, and everyday lives. Personal information has become an increasingly valuable commodity in the digital age.

At the same time, the abundance and persistence of personal data have elevated the risks to individuals' privacy. In the age of Big Data, the Internet of Things, Biometrics, and Artificial Intelligence, it is becoming increasingly difficult for individuals to fully comprehend, let alone control, how and for what purposes organizations collect, use, and disclose their personal information. Consumers are growing increasingly concerned about their privacy, making the need for strong privacy champions ever more acute.

With a veritable explosion of data breaches highlighted almost daily across the globe, and the introduction of heavy-handed privacy laws and regulatory frameworks, privacy has taken center stage for businesses. Businesses today are faced with increasing demands for privacy protections, ever-more complex regulations, and ongoing cybersecurity challenges that place heavy demands on scarce resources. Senior management and executives now acknowledge privacy as some of the biggest risks to the business.

Privacy, traditionally, has existed in a separate realm, resulting in an unintentional and problematic barrier drawn between the privacy team and the rest of the organization. With many regulatory frameworks to consider, building an all-encompassing data privacy program becomes increasingly challenging. Effective privacy protection is essential to maintaining consumer trust and enabling a robust and innovative digital economy in which individuals feel they may participate with confidence.

This book aims at helping organizations in establishing a unified, integrated, enterprise-wide privacy program. This book is aiming to help privacy leaders and professionals to bridge the privacy program and business strategies, transform legal terms and dead text to live and easy-to-understand essential requirements which organizations can easily implement, identify and prioritize privacy program gap initiatives and promote awareness and embed privacy into the everyday work of the agency and its staff.

First edition published 2023
by CRC Press
6000 Broken Sound Parkway NW, Suite 300, Boca Raton, FL 33487–2742

and by CRC Press
4 Park Square, Milton Park, Abingdon, Oxon, OX14 4RN

CRC Press is an imprint of Taylor & Francis Group, LLC

Library of Congress Cataloging-in-Publication Data
Names: Tang, Alan, (Information Security), author.
Title: Privacy in practice: establish and operationalize a holistic data privacy program/Alan Tang.
Description: First edition. | Boca Raton : CRC Press, 2023. | Series: Security, Audit and Leadership Series | Includes bibliographical references.
Identifiers: LCCN 2022041629 (print) | LCCN 2022041630 (ebook) | ISBN 9781032125466 (hardback) | ISBN 9781032125473 (paperback) | ISBN 9781003225089 (ebook)
Subjects: LCSH: Data protection. | Computer security. | Privacy, Right of. | Internet—Security measures.
Classification: LCC HF5548.37. T36 2023 (print) | LCC HF5548.37 (ebook) | DDC 658.4/78—dc23/eng/20220914
LC record available at https://lccn.loc.gov/2022041629
LC ebook record available at https://lccn.loc.gov/2022041630

ISBN: 978-1-032-12546-6 (hbk)
ISBN: 978-1-032-12547-3 (pbk)
ISBN: 978-1-003-22508-9 (ebk)

DOI: 10.1201/9781003225089

Contents

Foreword 1

Do you wish to kick-off an effective privacy program but are lost on where and how to start? This book is for you.

I first heard Dr. Alan Tang speak in Macau during the Asia Pacific Privacy Assembly forum in 2019 and was immediately impressed by his profound insights about data privacy and its implications for today's organizations. I learned much about the upcoming China data protection law when he discussed how the law came to be and its impact on companies operating within its reach. I also remember how he spoke knowledgeably about the societal, economic, and technological contexts of data privacy and protection. For someone coming from "industry", his grasp of data privacy's origins and contemporary issues and the fervor and flair he evangelized privacy's different and sometimes difficult aspects are marvelous.

I was excited that he finally put his thoughts and passion into writing to come up with this book. What I find remarkable about *Privacy in Practice* is the scope and breadth of Mr. Tang's knowledge on how to come up with an effective, holistic, and practical privacy program and the usefulness with which he presented it. Now, this is important. With the exponential growth of data privacy as a top-level concern, knowing how and where to start a practical privacy program is vital. But equally important, too, is ensuring that the materials are helpful in the real world.

I have seen the explosion of resources and references on establishing privacy programs useful for company DPOs and practitioners worldwide. But nothing comes close to an all-in-one "how to build a privacy program toolkit" than this book. I would know because as the first Privacy Commissioner of the Philippines, which is considered a newly formed volcano in data privacy, I never ceased to develop on my own and search for literature and references helpful for our companies to build their privacy programs.

After reading this book, I could say that the range of topics Dr. Alan Tang covered under one title, and the details he put are exceptional and presently unmatched. I confess that I have started using his manuscript as a reference in my work.

Dr. Tang has a nose for presenting what should genuinely matter for global privacy practitioners when building a holistic and operational privacy program. Contexts behind frameworks are vital to understanding where privacy legislations are based, where regulators are coming from and where future regulation is headed.

In this book, Dr. Tang will bring you back to where it all started. He laid the foundations of privacy principles brick by brick, how they developed slowly over time, and tracked how they spread all over the globe. His mastery of the critical privacy frameworks, sectoral rules, and laws that cast their influence worldwide shown in the book. That is why this book provides the answers to where most, if not all, of today's privacy developments stand. With Dr. Tang handholding you throughout your reading, he's handing you both a magnifying glass and a pair of binoculars as tools to chart an effective privacy program.

I learned a lot reading this book. As head of a DPA, I got to keep up with the rapid pace of privacy developments globally. A regulator's worst fear is being stumped when faced with tricky questions about global trends, practices, and cross-border privacy rules from company data protection officers and data subjects. I discovered Dr. Tang's book to be an excellent reference and useful as a map to help the reader navigate a privacy world that has become more complex. With this book as your handy companion, you will never be intimidated by privacy permutations that challenge even us, regulators.

As an elected member of the Global Privacy Assembly executive committee in 2019–2020, I had ringside seats on privacy development globally. I have witnessed the dramatic rise of more jurisdictions adopting privacy laws and starting their regimes. During that period, record fines were set in the EU, Canada, and the US, as more DPAs have stepped up in enforcing their privacy laws.

Notable, too, are the maturation of larger jurisdictions like Brazil and China. In Asia, there's the anticipation of more populous countries like India and Indonesia finally approving their privacy laws. Meanwhile, more established jurisdictions like New Zealand, Hong Kong, and Singapore have amended their laws to introduce more stringent measures to protect personal data.

All these are proof that the global data privacy momentum will not diminish. And with the patchwork of data privacy laws that have sprung up in recent years, finding your way around and steering your company away from business risks that now include hefty fines and penalties are becoming more challenging.

Your goal is to position your organization to be trusted by your clients, partners, customers, and importantly, by regulators. There is a single pathway, and that journey starts by implementing an effective privacy program to prove that your company deserves that trust.

You are fortunate to be holding on to Dr. Tang's book as your manual for building your privacy program. This book is a veritable toolbox for companies aiming to jumpstart their privacy program. It is a must-read and must-keep for company CEOs and members of the Board Directors and a companion for data protection officers and practitioners who wish to contribute to their companies' bottom line by treating data privacy and protection as a competitive differentiator.

The rules on personal data have changed but continue to develop at an unprecedented pace. As a result, you can rarely find the answers to many global privacy questions especially how to build a holistic and operational privacy program in one book. Fortunately, this book has finally arrived.

Raymund Enriquez Liboro
Former and First Privacy Commissioner for Philippines
August 1, 2022

Foreword 2

When Alan told me that he didn't set out to write a beach book, I think he forgot for a moment where I was sitting. Like so many folks in recent times, the two of us had not spoken in person for at least a few years and were having a video call to discuss this text. I looked out the window and chuckled.

Bermuda is a small place, and you often have a glimpse of a bay or the open ocean or can hear the crashing of waves on the volcanic rocks. To a certain extent, every book here becomes a beach book, whether it wants to or not.

As the first Privacy Commissioner for Bermuda, I have embraced this reality, turning to seaside analogies and nautical themes to explain the varied issues of privacy, data, and technology ethics. For example, we have designed a "Mid-Atlantic Privacy Compass" to describe our regulatory philosophy, and one of our office's key programs is a "P.I.N.K. Sandbox" to match our rose-colored beaches.

Alan's "Privacy in Practice" is most certainly not a beach book – nor should it be. The privacy and data protection issues confronted each day by anyone using a computer are not breezy. They are fundamental to the functioning of our communities.

Privacy helps our political structures to function by protecting freedoms of assembly and secret ballots. It enables our economies by helping us trust one another in online or other marketplaces where we do not know the other party. As we all are shown more and more "personalized content" and advertisements, we can see how data usage and privacy choices shape the information we receive – privacy supports the very integrity of our minds and decision-making. Protecting personal information against misuse is essential to maintaining our autonomy and self-determination. Hardly stuff to make you relax and fall asleep in the sun.

These issues are complex and changing quickly with each cycle of technological innovation or each new application for uses of information. As a regulator that is focused on proactive and constructive engagement with organizations to find mutual, win-win solutions, I firmly believe that the best way to protect individuals from the harm caused by misuse of their personal information is by convincing organizations, or "controllers," that it makes business sense to do so. Our own office has a running series we call "Privacy Means Business" to highlight how the practical application of data protection and data management programs can make organizations more efficient and profitable, all while better protecting their customers or employees.

Part of the task of privacy and data protection regulators is to make compliance with relevant laws easy – but thanks to the diversity of possible uses of data, that task is easier said than done. Here is where Alan comes in with the text you now hold. To tackle the challenging and unique issues that each organization faces, you need precisely the kind of checklists, refreshers, and quick reference tools you will find in these pages. This desk reference can be digested in bite-sized chunks, or searched, to find condensed explanations and briefings to give you the answers you need in the course of your work.

This book will not lull you to sleep like the sound of waves washing onto the shore – it will awaken you to the complexity of the rights and responsibilities created by legal regimes from around the world.

With that said, it may just help you relax after all to know that you have it, if needed, in your desk drawer.

Alexander White
Privacy Commissioner for Bermuda
10 July 2022

Preface

Privacy is not just the right to be left alone, but also the right to autonomy, control, and access to your personal data.

The employment of new technologies over the last three decades drives personal data to play an increasingly important role in our economies, societies, and everyday lives. In the digital age, various political, economic, social, and private activities of human civilization are linked or mapped to the digital space, or even directly realized in a digital manner, which will inevitably generate a massive data scale. Many of our traditional face-to-face interactions, such as banking, shopping, and social connections, are now taking place online. Personal information has become an increasingly valuable commodity in the digital age. According to the estimation of Statista, an international authoritative statistical agency, the global data volume has reached 47 zettabytes in 2020, and it is expected to reach 2,142 zettabytes by 2035.[1] The exponential explosion of data has become a strategic production factor in the digital age.

At the same time, the abundance and persistence of personal data have elevated the risks to individuals' privacy. In the age of Big Data, the Internet of Things, Biometrics, and Artificial Intelligence, it is becoming increasingly difficult for individuals to fully comprehend, let alone control, how and for what purposes organizations collect, use, and disclose their personal information. While more knowledge may lead to undeniable economic and social benefits, the availability of data and specialized analytics that are capable of linking seemingly anonymous information can paint an accurate picture of our private lives. The general public is much savvier about their data protection rights than they used to be. Consumers are growing increasingly concerned about their privacy, making the need for strong privacy champions ever more acute. The risks underline the need for more effective protection of privacy.

With a veritable explosion of data breaches highlighted almost daily across the globe, and the introduction of heavy-handed privacy laws and regulatory frameworks, privacy has taken center stage for businesses. Data protection laws exist to balance the rights of individuals to privacy and the ability of organizations to use data for their business. Data protection laws provide important rights for data subjects and the enforcement of such rights. Many data protection laws and regulations (i.e., EU GDPR) impose significant fines indicating the increasing importance of data protection as the value of personal data increases and the processing becomes even more sophisticated.

Businesses today are faced with increasing demands for privacy protections, ever-more complex regulations, and ongoing cybersecurity challenges that place heavy demands on scarce resources. Data privacy is increasingly on the tip of our tongues, regardless of company size or industry. Executives are increasingly concerned about data breaches. Senior management and executives now acknowledge privacy as some of the biggest risks to the business. With impending regulatory frameworks looming, business leaders find themselves scrambling to ensure that all bases are covered when it comes to data privacy. Privacy, traditionally, has existed in a separate realm, resulting in an unintentional and problematic barrier drawn between the privacy team and the rest of the organization. With many regulatory frameworks to consider, building an all-encompassing data privacy program becomes increasingly challenging.

Effective privacy protection is essential to maintaining consumer trust and enabling a robust and innovative digital economy in which individuals feel they may participate with confidence. Organizations that understand this and embrace a culture of privacy are those that will be most successful in this digital age.

This book is intended for the following audience from small, medium, large, and international organizations.

- Chief Privacy Officer/Privacy Officer
- Data Protection Officer
- Privacy professionals
- Chief Security Officer/Security Officer
- Risk Officer
- Business Leaders
- Professionals who want to gain knowledge in the privacy space

This book aims at helping organizations in establishing a unified, integrated, enterprise-wide privacy program that guides business units through providing privacy protection, maintaining privacy integrity, and offering protection measures during product development. This book is aiming to help privacy leaders and professionals to:

- Bridge the privacy program and business strategies. Demonstrate an understanding of the goals and strategies of the organization, and how the privacy program can support the business. Extend the privacy program beyond the privacy team or organizational function.
- Transform legal terms and dead text to live and easy-to-understand essential requirements which organizations can easily implement.
- Engage with business departments in an understanding of the scope of privacy within the context of the organization and build an environment that places privacy ownership in the hands of the business.
- Identify and prioritize privacy program gap initiatives. Establish and operationalize an actionable privacy program roadmap.
- Leverage privacy as a competitive advantage in streamlining how customer data flows through the organization. Shift the organization's view of privacy as the enemy of efficiency and innovation.
- Promote awareness and embed privacy into the everyday work of the agency and its staff.

Author

Dr. Alan (Chang Long) Tang is currently a Principal Research Director with Info-Tech Research Group. Dr. Tang has extensive experience devoted to privacy and security practices. He specializes in establishing and operationalizing risk-based and actionable privacy frameworks and programs in alignment with global privacy laws, regulations, and standards such as GDPR, CCPA/CPRA, PIPEDA, PIPL, LGPD, GAPP, ISO 27701, and NIST PF, etc. He believes in simplifying, automating, and scaling privacy controls to enable business growth.

Dr. Tang has firsthand experience in implementing an enterprise-wide, unified privacy framework and program for a Fortune 50 international company. The privacy framework has been implemented in 50+ countries through three phases. He has a strong history of working with business leaders in a wide range of privacy-related domains such as privacy strategy and roadmap, PIA and DPIA, privacy policies and procedures, privacy-by-design in SDLC, data subject rights assurance, data retention, data disclosure and sharing, data cross-border transfer, data security protection, privacy awareness training, data breach handling, etc.

Dr. Tang earned a PhD in information security and an MBA. Alan also holds numerous privacy and security designations including FIP, CIPP/E, CIPP/US/C, CIPM, CIPT, CISSP, CISA, PMP, and previously ISO27001LA and PCI DSS QSA.

Part 1

Privacy Basics and Landscape

This Part Covers the Following Topics:

- Privacy and Data Protection Key Concept
- A Brief History of Privacy
- Privacy Models and Common Principles
- Main Privacy Laws and Regulations
- Main Privacy Frameworks, Certifications and Codes of Conduct

DOI: 10.1201/9781003225089-1

1 Privacy Concept and a Brief History

This chapter is intended to help readers grasp the basic definitions of privacy, understand the brief history of privacy and be able to speak the privacy language.

This chapter covers the following topics:

- *Definition of privacy and data protection*
- *Definition of personal data*
- *Definition of sensitive personal data*
- *Timeline of privacy development*

1.1 NARRATIVES OF PRIVACY AND DATA PROTECTION

Culture Dependence

Privacy concepts and laws are culture dependent. People from different countries with diverse cultural backgrounds may have different views, interpretations, and perspectives on what is privacy. Privacy and data protection should not be studied without considering specific cultural, social, technological, and historical circumstances.

Professor Irwin Altman outlined his privacy regulation theory in *The Environment and Social Behavior* (1975) that privacy regulation theory has to do with the fact that people have different privacy standards at different times and in different contexts. For example, your definition of what constitutes "private information" in your relationship with your spouse is different than in your relationship with your children, and it's also different with your boss and coworkers.[2]

Since time immemorial, all cultures, all over the world, have had some understanding of privacy as a concept. Some codified it into laws, while others integrated it with religious beliefs. Privacy has been, and remains, the subject of rigorous academic study. Anthropology, sociology, psychology, history, and other disciplines have been looking into the concept and developing their definitions and models to describe Privacy.

Definitions of privacy have evolved over time, and our understanding of the concept is constantly changing. It is paramount that we understand not only privacy as a concept but privacy in context.

Privacy is not only about one individual

One of the commonly misunderstood facts is that your personal information implies that you are the only concerned party when it comes to sharing it. Privacy is as collective as it is personal. For instance, your DNA and other biometric data also carry substantial information about your family members, and their health and disease information.

Influential Narratives of Privacy

Although there is no one universally agreed definition of privacy, there are some representative narratives that influence and shape the landscape of privacy legislation and court cases as illustrated in Table 1.1.

In 1888, Thomas Cooley wrote in *A Treatise on the Law of Torts or the Wrongs Which Arise Independent of Contract* that people had a right to be let alone. Samuel D. Warren and Louis D. Brandeis elaborated on this concept in their seminal 1890 article in the Harvard Law Review, "The Right to Privacy." They argued that the common law's protection of property rights was moving

DOI: 10.1201/9781003225089-2

TABLE 1.1
Examples of the Definitions of Privacy

Narrative	Source
"A right to be let alone."	Thomas Cooley, A Treatise on the Law of Torts or the Wrongs Which Arise Independent of Contract (P16 and P29), 1888 Samuel Warren and Louis Brandeis, Harvard Law Review, 1890
"No one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence."	Article 12, United Nations Universal Declaration of Human Rights, 1948
"The right to respect for one's private and family life, home, and correspondence."	Article 8, European Convention on Human Rights, 1950
"The claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."	Alan Westin, Privacy and Freedom, 1968

toward the recognition of a right to be let alone. Their article inspired some state courts to begin interpreting the civil law of torts to protect a right of privacy.

Three years after the end of the World War II, the UN Universal Declaration of Human Rights was proclaimed on December 10, 1948, in Paris, set forth milestone standards for the treatment of all people. It has influenced European data protection laws and standards. Article 12 of the declaration is the focus on protecting people's private and family life, home, and correspondence. Everyone has the right to the protection of the law against such interference or attacks. The right to freedom of expression is set out in Article 19 (Right to free speech). And Article 29 (2) addresses that the rights are not absolute, and a balance should be struck.

The European Convention on Human Rights (ECHR, formally the Convention for the Protection of Human Rights and Fundamental Freedoms) is an international treaty to protect human rights and fundamental freedoms in Europe. Article 8 (Right to respect for private and family life) sets forth the principles listed to follow. Article 10 (Freedom of speech) protects the rights of freedom of expression and to share information and ideas across national boundaries; Article 10 (2) promotes balance between Article 8 and 10.

- Everyone has the right to respect for his/her private and family life, his/her home, and his/her correspondence.
- There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety, or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Different Aspects of Privacy

Although privacy can be defined in many ways, four main areas of privacy are of particular interest regarding data protection and privacy laws and practices: information privacy, bodily privacy, territorial privacy, and communications privacy[3] as described in Table 1.2. The distinction between these four types of privacy provides useful vehicle for making academic analysis, however, in many cases, individual's privacy interests could overlap.

In general, there are three actors that can intrude on an individual's privacy rights as listed in Table 1.3.[4]

TABLE 1.2
Four Types of Privacy

Type of privacy	Description
Information privacy	As defined by Alan F. Westin in *Privacy and Freedom* in 1968 that information privacy is "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." Examples of information privacy include identity documents (i.e., passports, driver's license), education and employment history, bank statements and financial transactions, family status, marriage status, trade union membership, etc.
Communications privacy	Communication privacy focuses on the protection of communication means, including email, postal mail, telephone conversations, fax, and other forms of communication behavior and means of communication.
Bodily privacy	Bodily privacy focuses on the protection of a person's physical existence and integrity from intrusion or offense. A person who deliberately physically infringes on the privacy of another person or his personal or interests is liable to the other person for infringement of his privacy if the intrusion is offensive to a reasonable person. Such intrusion or offense may take the form of a body scan and search, a blood test, or any form of genetic testing.
Territorial privacy	Territorial privacy focuses on the protection of people's physical environment and surrounding from others' invasion. The concept of the environment has evolved beyond home to include a broader notion such as workplace and public space, etc. Invasion of personal territorial privacy may take the form of video or audio monitoring and surveillance, physical search of the facility, etc.

TABLE 1.3
Three Actors That Might Intrude Individual's Privacy

Actor	Perspective	Description
Other individuals	Individual vs. other individuals	Protect an individual's privacy from intrusion from other individuals, such as a colleague, friend, neighbor, family member, random stranger, hacker, etc.
Organizations	Individual vs. organizations	Protect an individual's privacy from the intrusion from organizations or entities that can collect, use, and share personal data about an individual usually by providing products or services.
States	Individual vs. states	Protect an individual's privacy from intrusion from his or her own state or a foreign state that might monitor and track individual's behavior.

Figure 1.1 illustrates the high-level relationship among various aspects such as types of privacy and intrusion actors.

Privacy and Data Protection

The terms "privacy" and "data protection" are often used interchangeably. To me, there are some slight differences between privacy and data protection just like the two sides of a coin as shown in Figure 1.2. When you look at it, it represents different perspectives.

- From a data subject perspective, it is more about his or her rights, controllability, and assurance of privacy.
- From an organization (i.e., data controller or processor) perspective, it is more of the data protection side that requires and demonstrates the accountability to properly manage and protect personal data, such as the rules and safeguards applied under various laws and regulations to personal data.

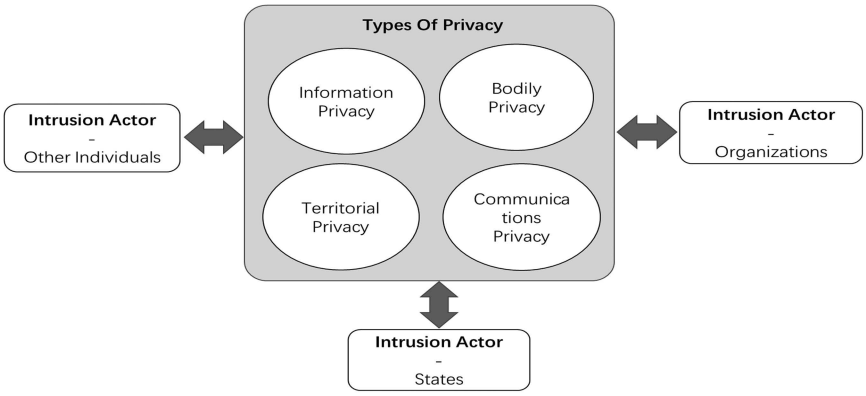


FIGURE 1.1 Relationship among types of privacy and intrusion actors.

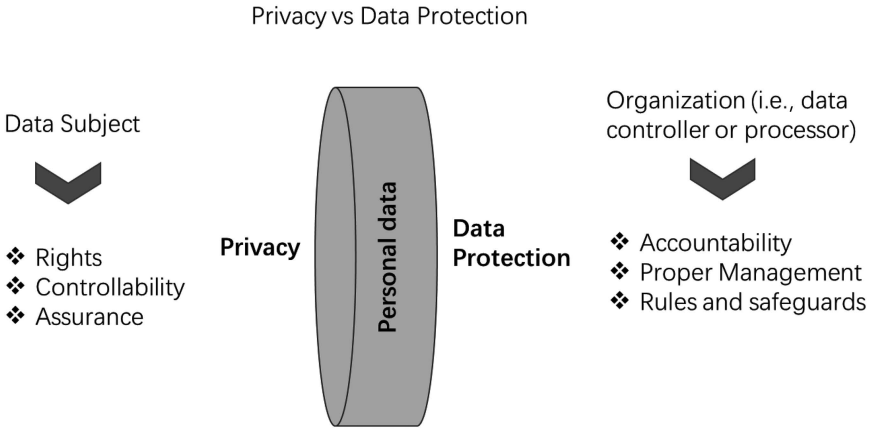


FIGURE 1.2 Privacy vs. data protection.

TABLE 1.4
Key Differences between Privacy and Confidentiality

	Privacy	Confidentiality
Focus	**Individuals**	**Data**
Attribute	Privacy is a right of a people or group of people.	Confidentiality is a property of data, any data, not just personal data.
Essential meaning	Privacy is personal choice. Privacy is a right to control access across a person's physical, decisional, informational, and dispositional dimensions.	Confidentiality is a professional obligation. Confidentiality is an agreement between the persons to maintain the secrecy of sensitive information and documents.
Protection	Protect an individual's personal information, space, body, and communications from intrusion from other individuals, organizations, and states.	Protect data from unauthorized access.

Privacy and Confidentiality

Privacy is mainly about people's rights and expectations. Confidentiality, on the other hand, is all about data. Table 1.4 illustrates the key differences.

1.2 PERSONAL DATA AND SENSITIVE PERSONAL DATA

1.2.1 Personal Data

Personal Data Definitions

You might have noticed that the definition of personal data varies from jurisdiction to jurisdiction in terms of the terms, nature, coverage, and scope. For instance, some regulations use personal data, however, other regulations use personal information. In this book, "personal data" and "personal information" will be deemed as the same and used interchangeably. Examples are listed in Table 1.5.

In a situation that an organization is operating in more than one jurisdiction that have different definitions of "personal information (data)" and "sensitive personal information", the agreed definitions should be adequate and consistent to reflect all legal contexts.

Core Elements of Personal Data

As illustrated by various definitions mentioned previously, most of the personal data definitions are substantially similar and cover the following four aspects as defined by the GPDR article 4(1).

TABLE 1.5
Examples of Personal Data Definition

Region	Regulation/Standard	Definition
EU	General Data Protection Regulation (GDPR)	Personal data means any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
US	Gramm-Leach-Bliley Act (GLBA)	Non-public Personal Information means personally identifiable financial information.
US	The Health Insurance Portability and Accountability Act (HIPAA)	PHI is any individually identifiable health information in any form. "Health information" means relating to any past, present, or future health condition or to health care or to payment for health care.
US	Family Educational Rights and Privacy Act of 1974 (FERPA)	Personally Identifiable Information: The term includes, but is not limited to— (a) The student's name (b) The name of the student's parent or other family members (c) The address of the student or student's family (d) A personal identifier, such as the student's social security number, student number, or biometric record (e) Other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name (f) Other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty (g) Information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates
US	The California Privacy Rights Act of 2020 (CPRA)	"Personal information" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household.

(*Continued*)

TABLE 1.5 (Continued)

Region	Regulation/Standard	Definition
US	Colorado Consumer Protection Act	(I) Personal information means a Colorado resident's first name or first initial and last name in combination with any one or more of the following data elements that relate to the resident, when the data elements are not encrypted, redacted, or secured by any other method rendering the name or the element unreadable or unusable: (A) Social security number (B) Driver's license number or identification card number (C) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial account (II) Personal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely distributed media
US	Connecticut Data Breach Law	Connecticut defines personal information as "an individual's first name or first initial and last name in combination with any one, or more, of the following data: (1) Social Security number [although Nevada specifically excludes the last four digits as PI]; (2) driver's license number or state identification card number; or (3) account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account."
US	DOJ Order 0904	Personally Identifiable Information: Information that can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth or mother's maiden name. DOJ information: Information that is owned, produced, controlled, protected by, or otherwise within the custody or responsibility of DOJ, including, without limitation, information related to DOJ programs or personnel. It includes, without limitation, information (1) provided by, generated by, or generated for DOJ, (2) provided to DOJ and in DOJ custody, and/or (3) managed or acquired by a DOJ contractor in connection with the performance of a contract. National security information: Information that has been determined (pursuant to Executive Order 12958 as amended by Executive Order 13292, or any successor order, or by the Atomic Energy Act of 1954, as amended) to require protection against unauthorized disclosure and is marked to indicate its classified status.
China	Personal Information Protection Law	Personal information is all kinds of information, recorded by electronic or other means, related to identified or identifiable natural persons, not including information after anonymization handling.
Canada	Personal Information Protection and Electronic Documents Act	Personal information means information about an identifiable individual.
Bermuda	Personal Information Protection Act 2016	Personal information means any information about an identified or identifiable individual.
Global	ISO/IEC 27018:2014(E)	Personally identifiable information (PII): any information that (a) can be used to identify the PII principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII principal.
US	NIST SP800–122	Personally Identifiable Information (PII) is any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Region	Regulation/Standard	Definition
China	GB/T 35273–2020	Personal information: any information that is recorded, electronically or otherwise, that can be used alone or in combination with other information to identify a natural person or reflect the activity of a natural person.
North America	NERC (North American Electric Reliability Corporation)	Personnel Information that identifies or could be used to identify a specific individual, or reveals personnel, financial, medical, or other personal information. Source: NERC Employee Code of Conduct
US	FERC (The Federal Energy Regulatory Commission)	Personally Identifiable Information includes information that is personal in nature, and which may be used to identify you (e.g., social security numbers, birthdates, and phone numbers). Source: FERC Administrative Policies
Japan	APPI	Previously, the APPI defined personal information as only the name, address, and date of birth. The amended APPI seeks to be more comprehensive by including any "personal identifier code", referring to biometric information (e.g., DNA sequences, fingerprints, facial appearance), specific identifier numbers (e.g., passport and driver's license, resident cards, "My Number"), other IDs uniquely assigned to an individual (e.g., health care cards, credit cards), and any codes the PPC might designate in the future as being equivalent to the prior categories. Note that for now, unlike the European General Data Protection Regulation (GDPR), the APPI only includes codes assigned to individuals, not to devices (e.g., IP addresses, mobile subscription identification numbers).

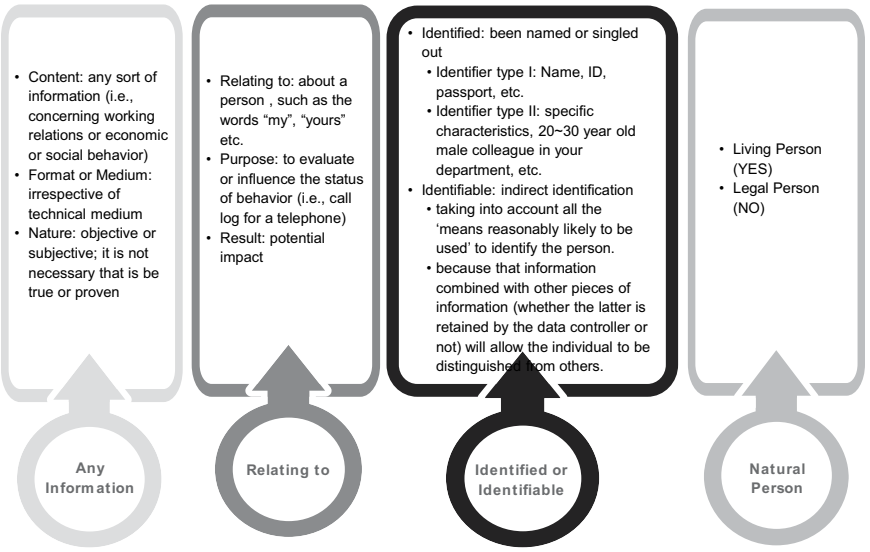


FIGURE 1.3 Four aspects of personal data.

Personal data is:

- **any information**
- **relating to**
- **an identified or identifiable**
- **natural person**

Figure 1.3 summarizes these four aspects providing a further explanation to help readers understand what each aspect entails.

Article 29 working party provides further information and context that I summarize next to help readers in making decisions on whether a piece of information is personal data.[103]

1) **Any information:** is understood to be literal. Information could be anything from a person's name to her location.
   - Content: the concept of personal data includes data providing any sort of information. The term "personal data" includes information touching the individual's private and family life, but also information regarding whatever types of activity are undertaken by the individual, like that concerning working relations or the economic or social behavior of the individual.
   - Format or medium: irrespective of the technical medium; information is available in whatever form, be it alphabetical, numerical, graphical, photographic, or acoustic, for example. It includes information kept on paper, as well as information stored in computer memory by means of binary code, or on a videotape, for instance.
   - Nature: objective or subjective; it doesn't need to be true or proven.
2) **Relating to:** refers to the information's purpose and impact on someone's privacy rights. Its juxtaposition with other content is also important. For example, a job title would not necessarily relate to a person, but a job title combined with a name likely would.
   - Content: Information "relates" to a person when it is "about" that person, and this has to be assessed in the light of all circumstances surrounding the case.
   - Purpose: taking into account all the circumstances surrounding the precise case, with the purpose to evaluate, treat in a certain way or influence the status or behavior of an individual. (i.e., call log for a telephone)
   - Result: data can be considered to "relate" to an individual because their use is likely to have an impact on a certain person's rights and interests, taking into account all the circumstances surrounding the precise case. It should be noted that it is not necessary that the potential result be a major impact. It is sufficient if the individual may be treated differently from other persons as a result of the processing of such data.
3) **Identified or identifiable:** "Identified" means that an individual person has been named or singled out—for example, by specific characteristics. And, as stated in Recital 26 of the GDPR, "Identifiable" refers to indirect identification, taking into account all the "means reasonably likely to be used" to identify the person.
   - Directly
   - Indirectly: In cases, where prima facie the extent of the identifiers available does not allow anyone to single out a particular person, that person might still be "identifiable" because that information combined with other pieces of information (whether the latter is retained by the data controller or not) will allow the individual to be distinguished from others (page 13).
4) **Natural person**: As stated in the GDPR, information must relate to a "natural person" for it to be considered personal data, which means that the information must be about a living, breathing person who is living. It doesn't include data in relation to "legal persons" (that is, corporations or other organizations with a separate legal status) or data in relation to public authorities. Figure 1.4 demonstrates the definition of natural person.

- Deceased Person
  - EU members take different approaches with respect to deceased persons:
    - Countries with regulations that do not cover personal data about deceased persons: Austria, Belgium, Bulgaria, Croatia, Cyprus, Finland, Germany, Greece, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, and Romania.
    - Countries with regulations that have limited obligations: the Czech Republic, Denmark (10Y after), Estonia (10Y/20Y-Minor), France, Hungary (5Y), Iceland

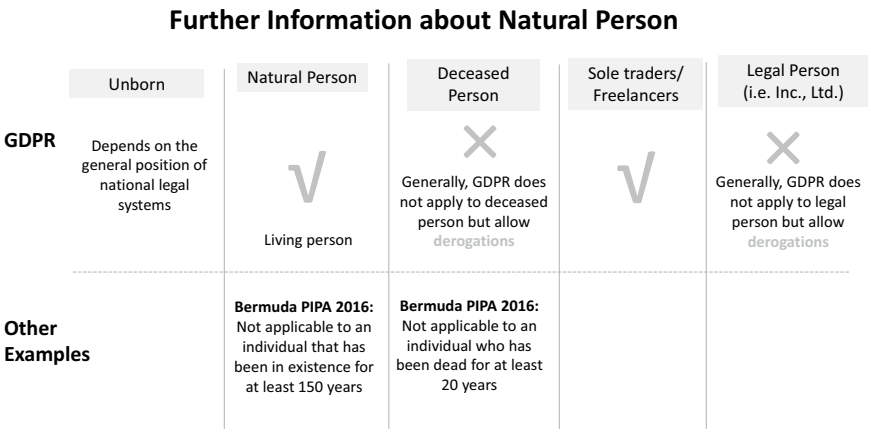


FIGURE 1.4 Definition of natural person.

(5Y or longer if confidential), Ireland (health data applies), Portugal (genetic data and health data apply).

- In terms of data subject rights request, Bulgaria, Hungary, Italy, Portugal, Slovakia, and Spain have each granted specific rights to heirs or family members of deceased persons, with respect to the processing of the deceased person's personal data (e.g., a deceased person's heirs may have the right to enforce the rights of access, rectification, or erasure, on behalf of that deceased person).
  - In Hungary, close relatives of the deceased or a person appointed by the data subject during his or her lifetime have the right to exercise data subject rights on behalf of the deceased.
  - In Italy, an agent of the deceased data subject can exercise data subjects on behalf of the deceased data subject.
  - In Spain, heirs or executors of the deceased data subject are entitled to exercise certain data subject rights (namely the right of access, the right of erasure and the right of rectification).
  - French law allows for data subjects to provide instructions for the management of their personal data after their death.
- Unborn children: The extent to which data protection rules may apply before birth depends on the general position of national legal systems about the protection of unborn children.
- Legal persons: As the definition of personal data refers to individuals (i.e., natural persons) information relating to legal persons is in principle not covered by the Directive, and the protection granted by it does not apply. However, certain data protection rules may still indirectly apply to information relating to businesses or to legal persons, in a number of circumstances.
- Sole traders: Data relating to sole traders (that is, people who run a business but not through a separate legal entity), employees, partners, and directors (where the information relates to them as individuals) may be personal data. For example, an employee's name within a corporate email address (such as paulsmith@xyz.com) will still be personal data, but the content of work emails will not necessarily be their personal data unless it "relates" to them or has an impact upon them.

Example: Systems IDs and passwords

- Self-selected system usernames are considered personal data. GDPR Article 4 articulates that "personal data" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person

is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

- In real-life practices, if you are allowed to select a system username, you may decide to use your public Twitter handle as your username. You may mention your Twitter ID on your Facebook or Google+ page or LinkedIn profile. Self-selected system usernames should be considered personal data because a site owner will not know if a person's self-selected usernames are the same as their public username.
- Regarding password, as a stand-alone data item, it does not belong to personal data. However, in actual business scenarios, account numbers and passwords are generally processed and treated together, that is, account numbers and passwords are usually treated together as personal data.

Example: IP addresses

An IP address is a unique address identifying a device connected to the Internet or a local network. A series of digits separated by periods—such as 123.45.67.89—can be either static or dynamic.

- Static IP address: A static IP address, manually configured, doesn't change. Static IP addresses are personal data when it comes to the user using the device to which the IP address has been assigned.
- Dynamic IP address: A dynamic IP address is automatically configured and assigned every time when a computing device is connected to a network. As such, it is temporary and changes. Dynamic IP addresses may be personal data under certain circumstances.

If a dynamic IP address can be combined with other data by the data controller or other interested parties—data held by the Internet service provider, such as, for example, the time of the connection and the pages that were visited—the address could be regarded as personal data.

Case Study: EU court decision—dynamic IP address, October 2017[5]

Dynamic IP addresses if they combine with other information could identify a person, and are considered personal data.

EU JUDGMENT OF THE COURT (Second Chamber)—19 October 2016. The Court of Justice of the European Union held that while Internet service providers assign dynamic IP addresses to users, website owners maintain records of using dynamic IP addresses to access their networks. Dynamic IP alone is not enough to identify a website user, but it can be combined with other data from the internet service provider to identify the user. Therefore, even if legal means are required to identify the data subject, dynamic IP addresses still meet the requirements for personal data in the EU Personal Data Protection Directive—identifiable and therefore personal data.

Case Study: US Virginia—License plate, 2018

The Supreme Court of Virginia ruled that a lawsuit challenging a police department's practice of keeping data from automated license plate readers for a year can move forward.

The year before, a judge dismissed a case filed by the American Civil Liberties Union in Fairfax County, ruling that a license plate doesn't contain personal information.

But the state's highest court reversed that ruling and sent the case back down to Circuit Court to determine whether the record-keeping process provides police with a "readily made" link to the vehicle's owner.

The court said if that link exists, then storage of the data is not exempt from Virginia's Government Data Collection and Dissemination Practices Act because the police "collected and retained personal information without any suspicion of criminal activity."

1.2.2 Sensitive Personal Data

Some personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create high or significant risks to fundamental rights and freedoms. Therefore, it requires a higher standard of protection. The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material, or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorized reversal of pseudonymization, or any other significant economic or social disadvantage.

Similar to the definitions of personal data, there is no universally agreed definition for sensitive personal data. While most privacy laws and regulations use the term "sensitive personal information", GDPR does not specially call out sensitive personal data, but the article (9) articulates special categories of personal data.

In general, sensitive personal data is a type of personal data that:

- **Personal data revealing . . .**
  - ✓ Racial/ethnic origin, political opinions, religious/philosophical beliefs, trade union membership
- **For the purpose of uniquely identifying a natural person**
  - ✓ Genetic data
  - ✓ Biometric data
- **Data concerning . . .**
  - ✓ Health, sex life, sexual orientation
- Note: Under the HR circumstance, the listing of spouses only reveals marital status not sex life.
- **Data relating to . . .**
  - ✓ Criminal convictions, offenses, security measures

Table 1.6 lists some exemplar definitions of sensitive personal information.

Relationship diagram

Based on GDPR, I built a relationship diagram illustrating different types of personal data with various sensitivity as shown in Figure 1.5.

1.3 TIMELINE OF PRIVACY DEVELOPMENT

The social concept of privacy is rooted in some of the oldest religions, texts, and cultures. Culturally, privacy is mentioned in early developed societies from classical Greece to ancient China. For example, privacy is recognized in the Bible, Jewish law, Quran, and the Analects.

TABLE 1.6
Examples of Sensitive Personal Data Definition

Region	Regulation/ Standard	Definition
EU	General Data Protection Regulation (GDPR)	Special categories of personal data: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.
France	Data Protection Act & Implementing Decree	Collecting data about a person's health and sex life and data that directly or indirectly reflect a person's racial, political, philosophical, religious views or trade union membership is prohibited.
Germany	Federal Data Protection Act	Race, political opinions, religious and philosophical beliefs, union membership, health, and sexuality.
US	CPRA (The California Privacy Rights Act of 2020)	"Sensitive personal Information" means (1) personal information that reveals (A) a consumer's social security, driver's license, state Identification card, or passport number; (B) a consumer's account log-in, financial account, debit card, or credit card number. In combination with any required security or access code, password, or credentials allowing access to an account; (C) a consumer's precise geolocation; (D) a consumer's racial or ethnic origin, religious or philosophical beliefs, or union membership; (E) the contents of a consumer's mall, email, and text messages, unless the business is the Intended recipient of the communication; (F) a consumer's genetic data; and (2)(A) the processing of biometric Information for the purpose of uniquely identifying a consumer; (B) personal Information collected and analyzed concerning a consumer's health; or (C) personal Information collected and analyzed concerning a consumer's sex life or sexual orientation. Sensitive personal Information that is "publicly available" pursuant to paragraph (2) of subdivision (v) of Section 1798.140 shall not be considered sensitive personal Information or personal information.
US	Gramm-Leach-Bliley Act (GLBA)	Non-public Personal Information means personally identifiable financial information.
US	Colorado Privacy Act	"Sensitive data" means: (a) personal data revealing racial or ethnic origin, religious beliefs, a mental or physical health condition or diagnosis, sex life or sexual orientation, or citizenship or citizenship status. (b) genetic or biometric data that may be processed for the purpose of uniquely identifying an individual; or (c) personal data from a known child.
China	GB/T 35273–2020	Personal sensitive information: Once leaked, illegally provided, or abused, personal information may endanger personal and property safety and easily lead to damage to personal reputation, physical and mental health, or discriminatory treatment.
Australia	Privacy Act	Race, political opinions, political group membership, religious beliefs, philosophical beliefs, union membership, sexual orientation, criminal records, health information, genetic information, biometric information, and biometric templates.
Japan	Guidelines for the Protection of Personal Information in the Financial Sector	There is no definition of sensitive personal data in the Japanese Personal Data Protection Law, but the "Guidelines for the Protection of Personal Information in the Financial Sector" stipulates that the scope of sensitive personal data includes: political opinions, religious beliefs, trade union membership, race, family origin, legal residence, medical records, sex life, criminal records.
Argentina	Personal Data Protection Act 2000	Sensitive data: Personal data revealing racial and ethnic origin, political opinions, religious, philosophical, or moral beliefs, labor union membership, and information concerning health conditions or sexual habits or behavior.

Region	Regulation/ Standard	Definition
Bermuda	Personal Information Protection Act 2016	"Sensitive personal information" means any personal information relating to an individual's place of origin, race, color, national or ethnic origin, sex, sexual orientation, sexual life, marital status, physical or mental disability, physical or mental health, family status, religious beliefs, political opinions, trade union membership, biometric information, or genetic information.

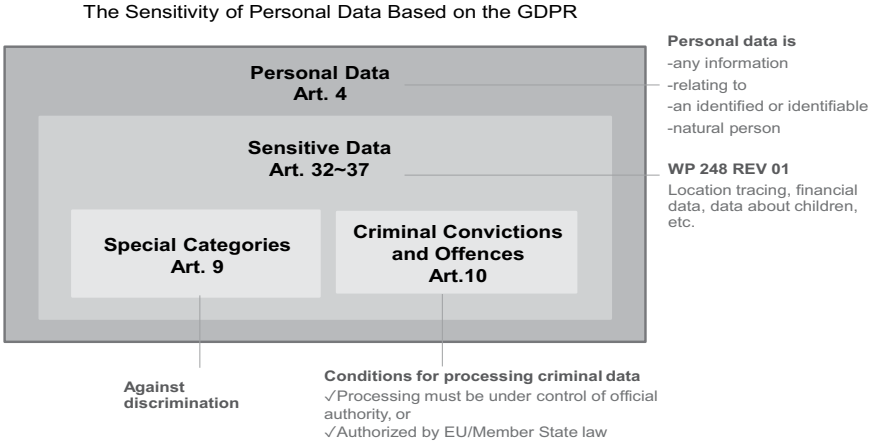


FIGURE 1.5 The sensitivity of personal data based on the GDPR.

From a privacy development timeline perspective, I think there are four main periods. The timeline that is described in Figure 1.6 illustrates the development of privacy from concept, social, and regulation development perspectives.

- Pre-Contemporary (1300s~1870s)
- Privacy 1.0: From Concept to Declaration (1880s~1950s)
- Privacy 2.0: From Principles to Regulations (1960s~2000s)
- Privacy 3.0: From Obligations to Advantages (2010s~Now)

1.3.1 Pre-Contemporary

The legal protection of privacy rights has a far-reaching history. It began in England in 1361 with the Justices of the Peace Act. This act included provisions calling for the arrest of "peeping Toms" and eavesdroppers.

In 1765, British Lord Camden struck down a warrant to enter and seize papers from a home and, in so doing, wrote,

> we can safely say there is no law in this country to justify the defendants in what they have done; if there was, it would destroy all the comforts of society, for papers are often the dearest property any man can have.

Parliamentarian William Pitt shared this view, writing that

> the poorest man may in his cottage bid defiance to all the force of the Crown. It may be frail: its roof may shake; the wind may blow through it; the storms may enter; the rain may enter—but the King of England cannot enter; all his forces dare not cross the threshold of the ruined tenement.

FIGURE 1.6 Timeline of privacy and data protection development.

In the following centuries, other European countries advanced more particularized privacy protections. The Swedish Parliament enacted the Access to Public Records Act in 1776, requiring that information held by the government be used for legitimate purposes. In 1858, France prohibited the publication of private facts, with violators of the prohibition subject to strict fines.

In the United States, the fourth amendment holds: The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched.

1.3.2 Privacy 1.0: From Concept to Declaration

In 1888, Thomas M. Cooley, justice, and later Chief justice of the Michigan Supreme Court, writes: "A Treatise on the Low of Torts or the Wrongs Which Arise Independently of Contract."

On December 15, 1890, two years after Cooley's writings, two brilliant young lawyers, Samuel D. Warren and Louis D. Brandeis, published in the Harvard Law Review an article titled "The Right to Privacy." Louis D. Brandeis eventually becomes a Supreme Court Justice. In 1902, Roberson v. The Rochester Folding Box Company antiprivacy judgment gave rise to sections 50 and 51 of New York State's Civil Rights Law. In 1939, The American Law Institute's first revision of Restatement of Torts included privacy concepts. The first modern international privacy law appeared in 1948, as Article 12 of the Universal Declaration of Human Rights. It was proclaimed on December 10 in Paris, with the wounds of the Second World War still fresh. It is a powerful document, drafted by representatives from all over the world hoping for a fresh, and less bloody start. In 1950, The European Convention on Human Rights is adopted, including Article 8, an expanded right to privacy.

Universal Declaration of Human Rights (^{UD}HR) December 10, 1948.

- Non-binding instrument, UDHR setup set forth milestone standards for the treatment of all people.
- It has influenced European data protection laws and standards.
- **Article 12** (Right to privacy)—No one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.
- The right to freedom of expression is set out in Article 19 (Right to free speech).
- Article 29 (2) (Balance) addresses that the rights are not absolute, and a balance should be struck.

European Convention on Human Rights (ECHR, enforced in 1953)

- It is an international treaty to protect human rights and fundamental freedoms, which can be enforced by the European Court of Human Rights in Strasburg. All Council of Europe member states have ratified the convention. It is one of the key documents for enforcing fundamental human rights in Europe and worldwide.
- **Article 8** (Privacy)—Right to respect for private and family life: Everyone has the right to respect for his private and family life, his home, and his correspondence.
- Article 10 (Freedom of speech), which protects the rights of freedom of expression and to share information and ideas across national boundaries.
- Article 10 (2) (Balance), which promotes balance between Articles 8 and 10.

Social, Economic and Technical Context:

- World War One and Two
- Rise in trans-border trade

1.3.3 Privacy 2.0: From Principles to Regulations

In 1970, The first modern privacy law was in Hesse, Germany. In 1973, The first national privacy law was in Sweden. Sweden passed the Data Act ("Datalagen," 1973), considered to be the first national data protection law. This law, which was fairly conservative by today's standards, governed how personally identifiable information was processed in computerized registers; it established a data protection authority with the ominous name "The Data Inspection Board," which would issue permits before a new personal data register could operate and determine specific conditions for its operation. The law has since been superseded by the European General Data Protection Regulation. Fair Information Practice (FTC FIPs) was initially proposed and named by the US Secretary's Advisory Committee on Automated Personal Data Systems in a 1973 report, "Records, Computers, and the Rights of Citizens", issued in response to the growing use of automated data systems

containing information about individuals. The central contribution of the Advisory Committee was the development of a code of fair information practice for automated personal data systems. The Privacy Protection Study Commission also may have contributed to the development of FIPs principles in its 1977 report, Personal Privacy in an Information Society. FIPs are the main reference of many other privacy protection frameworks such as Convention 108, OECD, etc. In 1977, The American Law Institute again revised the Restatement of Torts to include modern privacy concepts.

In 1980, The Organization for Economic Cooperation and Development (OECD) issued its first guidelines on data privacy protection. The OECD guidelines are recommendations from governments to multinational enterprises on responsible business conduct. They are guidelines for the protection of privacy and transborder flows of personal data. It is aimed to enable data flows and protect personal data. This membership extends outside of Europe and is not legally binding. The principles introduced were data quality principle, purpose specification, collection limitation, use limitation, openness, individual participation, security safeguards, and accountability. The guidelines were updated in 2013.

In 1981, The Council of Europe adopted Treaty 108: Convention for the protection of individuals with regard to automatic processing of personal data. The convention 108 or Council of Europe Convention is for the protection of individuals regarding the automatic processing of personal data.

In the late 1980s, difficulties with Convention 108 were becoming apparent. Only a small number of states had ratified it, and even those had adopted a fragmented approach. In the 1990s, the European Commission proposed the introduction of a dedicated directive. The principles contained in Convention 108 were used as a benchmark for the EU Data Protection Directive (95/46/EC). Operationally, the Directive set out general data protection principles and obligations, requiring EU member states to transpose and implement them.

From the 1970s to 2010, the globalization of the world economy and e-commerce has grown exponentially. The wide adoption and application of direct marketing, telemarketing, data mining, the Internet, personal computers, smartphones, big data, and social media raised a huge amount of privacy concerns. The capability to access data and share data from anywhere, on any device and at any time increased users' privacy risks. The enforcement of data privacy laws has picked up. In Europe, data protection authorities have increased their audit activities and issued fines.

Social, Economic, and Technical Context:

- The increase in international trade
- Development and use of direct marketing, telemarketing, data mining, Internet, personal computers, e-commerce, smartphones, etc.
- The increase in the amount of information
- Increasing demand for sharing personal information
- Conflict between national privacy rights and international free trade increased
- Legislation aiming to control the use of personal data by government agencies and large companies

1.3.4 Privacy 3.0: From Obligations to Advantages

Since 2013, former US spy contractor Edward Snowden's revelations about widespread surveillance of online communication have reverberated in recent years, sparking an international conversation on digital privacy.

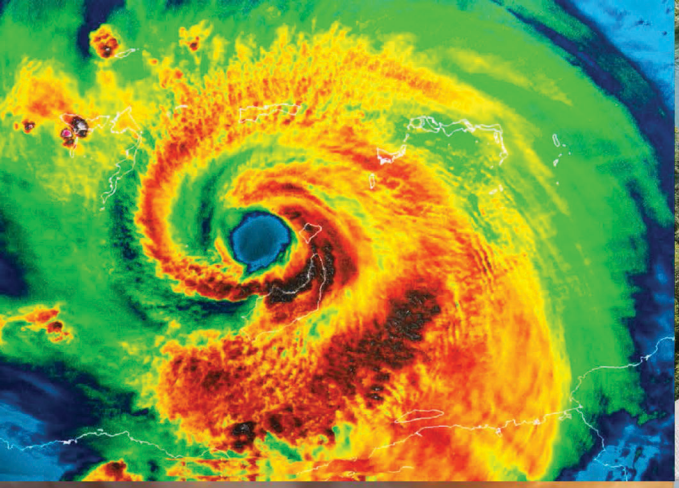
In 2014, the European Union Court of justice ruled that EU law grants EU citizens "the right to be forgotten" from search engines.

Countries are embracing broader digital strategies (i.e., Industry 4.0), which make privacy protection an integral part of people's digital life. Protecting the privacy and the rights and freedoms of individuals without creating any barriers to trade and allowing the uninterrupted flow of personal

data across national frontiers. At the same time, the Snowden case (2013) reminded us of individuals' privacy rights are facing tremendous threats from government surveillance.

Social, Economic, and Technical Context:

- Digital Strategy
- Industry 4.0
- Advanced technologies, AI, Big Data, IoT, etc.
- Proliferation of social media
- Privacy protection is an integral part of people's digital life
- Widespread surveillance of online communication from government agencies
- Data subjects demand more rights (i.e., right to be forgotten)



RIDING THE WAVE

APPLYING PROJECT MANAGEMENT SCIENCE IN THE FIELD OF EMERGENCY MANAGEMENT

ANDREW BOYARSKY

CRC Press
Taylor & Francis Group

Riding the Wave

Emergency managers and public safety professionals are more frequently being called on to address increasingly challenging and complex critical incidents, with a wider variety and intensity of hazards, threats, and community vulnerabilities. Much of the work that falls into the scope of emergency managers – prevention, preparedness, mitigation – is "blue sky planning" and can be contained and effectively managed within projects. This book provides a foundational project management methodology relevant to emergency management practice and explains and demonstrates how project management can be applied in the context of emergency and public safety organizations.

Special features include:

- an initial focus on risk assessment and identification of mitigation and response planning measures;
- a clear set of better practices, using a diverse set of examples relevant to today's emergency environment, from projects to develop emergency response exercises to application development to hazard mitigation;
- a framework for managing projects at a strategic level and how to incorporate this into an organization's program, as well as how to develop and manage an emergency program and project portfolio; and
- suitability as both a hands-on training guide for emergency management programs and a textbook for academic emergency management programs.

This book is intended for emergency managers and public safety professionals who are responsible for developing emergency programs and plans, including training courses, job aids, computer applications and new technology, developing exercises, and for implementing these plans and components in response to an emergency event. This audience includes managers in emergency and first response functions such as fire protection, law enforcement and public safety, emergency medical services, public health and healthcare, sanitation, public works, business continuity managers, crisis managers, and all managers in emergency support functions as described by FEMA. This would include those who have responsibility for emergency management functions, even without the related title.

Andrew Boyarsky, MSM, PMP, CBCP, cABCF, is President of Pinnacle Performance Management, and an emergency management and disaster recovery specialist with 30 years of experience in project management and 23 years in emergency management, business continuity, and disaster recovery. He is Clinical Associate Professor and teaches at NYU, John Jay College of Criminal Justice, and at Yeshiva University. In the early 1990s, he developed and managed large-scale emergency medical and mass care response projects overseas in the former Yugoslavia and in the Caucasus with the International Federation of the Red Cross and Red Crescent Societies and Catholic Relief Services/ Caritas Internationalis. From 2007 to 2016 Boyarsky was Project Manager for Coastal Storm Plan Training working on behalf of the NYC Office of Emergency Management, responsible for training over 30,000 city staff for emergency sheltering operations. This included managing additional training programs in logistics, recovery, special medical needs, and disability, access, functional needs, and pandemic response.

His clients have included FEMA, the Regional Catastrophic Planning Team of NY-NJ-CT-PA, New York City Office of Emergency Management, New York City Health Department, Los Angeles Emergency Management Department, Baltimore City Health Department, Westchester County (NY) Office of Emergency Management, and the NYC Human Resources Administration.

He has a B.A. from Johns Hopkins University, Masters in the Science of Management from the Hult International School of Business (formerly the Arthur D. Little School of Management), and earned his PMP certification in 2003, CBCP in 2019, and cABCF in 2020. He also hosts a podcast series, Riding the Wave: Project Management for Emergency Managers, and volunteers with the Community Emergency Response Team in South Orange, NJ, where he resides with his family.

Designed cover image: ©Shutterstock

First edition published 2024
by CRC Press
2385 NW Executive Center Drive, Suite 320, Boca Raton FL 33431

and by CRC Press
4 Park Square, Milton Park, Abingdon, Oxon, OX14 4RN

CRC Press is an imprint of Taylor & Francis Group, LLC

ISBN: 9781032062853 (hbk)
ISBN: 9781032062860 (pbk)
ISBN: 9781003201557 (ebk)

DOI: 10.1201/ 9781003201557

Typeset in Sabon
by Newgen Publishing UK

Contents

Preface

> When the situation was manageable it was neglected, and now that it is thoroughly out of hand, we apply too late the remedies which then might have effected a cure. There is nothing new in the story. It is as old as the Sibylline books. It falls into that long, dismal catalogue of the fruitlessness of experience and the confirmed unteachability of mankind. Want of foresight, unwillingness to act when action would be simple and effective, lack of clear thinking, confusion of counsel until the emergency comes, until self-preservation strikes its jarring gong—these are the features which constitute the endless repetition of history.
>
> *Winston Churchill, House of Commons, May 2, 1935*

We live in a VUCA[1] world, one that is filled with volatility, uncertainty, complexity, and with a sense of ambiguity as to where we may be headed, whether on a local or global community level. Let's face it, you don't need to look too far to see these signs that are creating this environment: natural hazards, human-caused threats, social and political strife, technological complexities, and financial and economic instability. Just read the news headlines to witness the manifestations. There are wildfires in the Western North America and Canada, widespread flooding in the Midwest and South Asia, increasing intensity of tropical cyclones, and tornadic activity spreading well beyond its typical range.

Roughly 12 years ago I had the opportunity to work on an environmental literacy course for the City University of New York. While conducting research for the course, one of the key points was the idea of the "Tipping Point".[2] This is where we move beyond the "Point of No Return" with increased global warming into runaway climate change with very unstable and extreme weather patterns. The very sad truth is that we are now beyond that tipping point. While the alarm bells were sounding loud and clear over a decade ago, the situation has worsened, with no signs of any improvement. The recent report by the Intergovernmental Panel on Climate Change (IPCC)[3] indicates that we are 1°C (roughly 1.8°F) above pre-industrial levels and will arrive at 1.5°C by 2030. This is a little more than ten years away as of this writing. Yet, we are already witnessing these extreme weather phenomena.

Being in the middle of this emerging phenomena makes it challenging at best to understand what is happening. What we commonly refer to as climate change is certainly having a destabilizing effect on weather patterns and consequent impacts on our environment. Human settlement and consumption are exacerbating the situation, not only in the

green-house gases that are emitted, but in the ways in which we interact with our environment. Here are just some examples:

- An extended wildfire season, moving from five months in the 1970s to now year-round; increased temperatures are causing severe drought, melting mountain snow packs earlier and leaving more areas exposed to burning. The Marshall Fire in Boulder, Colorado, in December 2021 is a clear example of this, causing over $500 million in damage to a major suburban community.[4]
- Increasing ocean water temperatures lead to greater evaporation and conditions that spawn and sustain larger storms (hurricanes/typhoons), monsoons, rainstorms, microbursts, etc.; this is true not only in the Western hemisphere but also in the Eastern hemisphere – witness the massive flooding in South Asia, displacing many millions of inhabitants. Similar flooding has been impacting the United States: the Mississippi River and Tennessee Valley in the past decade, just to name a few examples.
- Equally disturbing, increasing ocean temperatures are disrupting ecosystems, reducing ocean plant and animal life; corals are disappearing at an alarming rate and house numerous coastal fish populations.
- Season creep, wherein plants bloom earlier causing some species to come out earlier, leaves other species unable to compensate (what might be called a "late to dinner" effect). This has led to some animal populations beginning to collapse: migratory birds, insects, deer.
- Increasing development and hardscaping along river fronts and coastal areas have reduced natural watersheds and increased the extent and severity of flooding levels. As a clear example of this, Florida once was all wetlands, a giant peninsula of marshes, swamp, and grasslands, with a healthy ecosystem. We know the story; the swamp was dredged, water management put in place, and what we know as the Sun and Gold coasts, filled with resort communities, retirement homes and buildings, golf courses, etc. grew exponentially. But Mother Nature has a way of taking back what is rightfully hers.
- A similar trend is happening in the forested and mountain areas of the western United States; housing developments are pushing further into forested areas (Wildland Urban Interface or WUI), increasing their risk exposures to wildfires. While the doctrine of fire suppression by the US Fire Service was called into question and the FLAME Act was designed to address the shortage in resources in battling wildfires, we still see development unabated in western US states.
- Encroachment into corners of the globe where humans consume and trade in wild animals and comingling species where viruses can transmit and mix to foster greater potential for pathogens which can threaten human lives. The spread of Ebola and Monkeypox are the clearest examples of this type of pathogenic spread.

Our political structures are currently ill equipped to fully address the scope and scale of these threats and impacts to the environment. While some political leaders at the national and regional levels are tackling this challenge head on (a good example is the 100 resilient cities program[5]), other political leaders are reluctant to take the dramatic steps to reduce our common carbon footprint and, furthermore, to invest what is necessary in the immediate future for robust mitigation measures against natural hazards, such as flood barriers/

sea walls, levees, storm cellars (for tornados), seismic retrofitting (for earthquake), and forest maintenance, and establishing tougher building codes and zoning restrictions. Many of these measures are unpopular, as they do not show any clear, immediate "Return on Investment" and require political will and fortitude, moreover, and broad social support in the face of business development interests, which is why these efforts are often stymied.

We can see that our legal frameworks are strained and, at times, frayed by the advent of new technologies and perils, and our failure to harness them through legal and regulatory means: blockchain (e.g. unregulated cross-border currencies such as Bitcoin), the dark web, and the Internet of Things (IoT), just to name a few. On the social front, our natural, local community structures, supported by government, community organizations, and faith-based communities are weakened as our "24hrs./365 day/year, always-on" culture leaves little time for us to attend to immediate, long-term local issues and to connect across traditional local community and faith-based groups. With an increasingly transient society, it is challenging to muster a sense of community in order to gain consensus around concrete measures to deal with the impacts of climate change. Civil society has been further balkanized by the forces of political extremism and proliferation of social media as a primary source of news,[6] where groups create narrow, echo chambers for their own lines of thought without a strong consensus of what we see as a "common operating picture" of the potential challenges we face.

We are in great need of substantial measures along the panoply of risk responses to address the potential impacts of the threats and hazards that we face. In the absence of meaningful prevention and mitigation measures to eliminate or reduce vulnerability to risk impacts, professionals in emergency management and public safety will be called upon to address these perils and their consequences to protect and safeguard our communities.

NOTES

1 VUCA is believed to have been developed as a term at the US Army War College and is based on the management theories of Warren Benis and Burt Nanus. See: http://usawc.libanswers.com/faq/84869

2 Beyond the Point of No Return, December 12, 2007, See: www.heatisonline.org/contentserver/objecthandlers/index.cfm?ID=6752&method=full#_edn1; for a short video on the subject, see: http://wakeupfreakout.org/film/tipping.html

3 See www.ipcc.ch/sr15/chapter/summary-for-policy-makers/

4 As many as 600 homes lost, six people injured as Marshall fire quickly spreads across Boulder County. The Colorado Sun. Boulder, Colorado. December 30, 2021. Retrieved January 1, 2022. https://coloradosun.com/2021/12/30/boulder-grass-fire-evacuations/

5 See www.100resilientcities.org/

6 Experts Say the 'New Normal' in 2025 will be Far More Tech-Driven, Presenting More Big Challenges, *Pew Research Center, Internet and Technology,* February 18, 2021 www.pewresearch.org/internet/2021/02/18/emerging-change/

Part I

Setting Up the Basecamp for Projects

Chapter 1

The Accidental Project Manager

BAPTISM BY FIRE – FORMER YUGOSLAVIA AND THE MAP

In March of 1993 I landed on the ground in Zagreb, the national capital of Croatia. Croatia and neighboring Bosnia-Herzegovina were embroiled in brutal and bloody civil wars that had ensued after the break-up of Yugoslavia during 1991–1992. I was placed in charge of a medical assistance project to provide support for the medical needs of refugees and displaced persons in Croatia. Before my arrival, I had spent three days of orientation at the organization's headquarters in Baltimore, MD[1] and had read up prior to that on the Balkans' history, culture, and what led up to the war. Armed with this and an undergraduate degree in international relations, as well as some experience working in Eastern Europe, I felt ready to take on this new emergency humanitarian mission.

My taxi pulled up to the low whitewashed building just off the square of the main cathedral in Zagreb, where I emptied myself and all my baggage into the vestibule. At the door I was greeted by Sister Annamaria Šimić,[2] a petite, smiling nun who was born in Northern Bosnia. While short of stature, she made up for it in energy and fortitude. Once I had a chance to get settled in my hotel, our initial task at hand would be to look for office space.

I would not even get a chance to get my bags unpacked when I was immediately presented with my first urgent request; there were two refugees in the hospital with leukemia, whose doctors had submitted a list of needed medicines for their treatment. My project was not even operational, and I had a decision thrust upon me. The total cost between these two would have been about $60,000, a significant chunk of the $3.6 million budget I had to spend on pharmaceuticals. If I did agree to cover the cost, then at this rate of spending the project might wind up quickly exhausting the budget while covering a small number of needs. If I did nothing and the medicines were not provided, the odds were that these two young people might not survive.

That evening I called the US Embassy since the US State Department was the funding agent for the aid grant.[3] I figured that someone there could offer some guidance with this situation. It was the weekend, and my call was transferred to a duty officer who, after asking me the particulars of the patient cases, said there was little that he could do to help and then offered little encouragement by adding "I wouldn't want to be in your shoes". "Thanks" I thought.

What I did not realize at the time was that I was presented with a problem of project scope. If I decided to go the route of helping the few with acute medical needs such as

DOI: 10.1201/9781003201557-2

leukemia, then the project would have a limited reach in beneficiary numbers and most likely a shorter duration and geographical reach due to the limited number of hospitals in the country. If, on the other hand, I purchased inexpensive medicines and medical supplies, then the project might reach a broader population of refugees and displaced persons in the country. However, quick calculation of the average dollar per beneficiary would yield roughly $7.2 per beneficiary, a piddling amount even in war-torn Croatia. The solution clearly was somewhere in between the two options if the project was to have any significant impact.

Whatever course of action I chose, I still needed to come to a decision. Not making a decision was still a decision, with consequences attached. I decided to seek a private donation through my organization and asked the hospital to describe the two cases, respecting the privacy of the two patients, and submitted this along with an urgent request with a list of specific medicines and approximate cost to our headquarters. This request was replicated to the broader network of charities we were affiliated with, and in due time a donation was made for one of the cases; one patient had a positive prognosis, while the other's was negative and, unfortunately, was unlikely to survive. This was also among one of my first lessons; the project was not going to save all of the targeted beneficiaries, and not every outcome was going to be an unmitigated success. In a major disaster situation, including the impacts of a terrible civil war, the mission of the emergency manager is to do the greatest good for the largest number of people.

Amid all of the project documentation I had lugged around with me was a six-page project plan and a stack of organizational and US Government grant regulations and guidelines that stood about a foot high. The six-page project plan lay on the right side of the desk and provided no practical guidance as to how to clearly execute the project. The documentation on the left side of the desk appeared rather daunting and unlikely to yield anything helpful. Upon seeking advice from the head office as to what I should do, I was told: "read through all of the regulations and the project plan and decide on the appropriate course of action". After reading the first ten pages of the government regulations and realizing there was scant guidance as to my specific project or the operational environment—a civil war zone—I decided my logical course of action would be to use the six-page project proposal as my general guidance and my common sense to plan and execute the project. When I had time later on, I would read through the regulations for any relevant guidance. This proved to be the wisest choice. Expediency and practicality trumped administrative bureaucracy.

In those first few days, I realized that I had to have a better gauge of the scope of my project and settled on the idea of assessing the medical needs of the refugees and displaced persons in Croatia. My first stop was with the Ministry of Health where I met with the Deputy Minister of Health. His first question that he asked was "What can I get for you?". In my youthful haste, I rattled off a list of data points that I needed: locations of high-density refugee and displaced populations (DP), refugee and DP camps, clinics and medical stations serving mostly refugees and displaced persons,[4] health surveillance data, morbidity and mortality data, etc. He waited until I was done and then politely asked with a smile "I meant coffee, tea, or juice". I quickly realized that I had a lot to learn about my communication style and the culture of the country I was in. This was major lesson number two; I would have to adapt to the local working environment and the culture. This

was particularly complicated by the fact that there were many regional differences, as well as political and social considerations, not the least of which was that, quite frankly, I was working in a war zone.

The truth became apparent in that first meeting with the Ministry of Health that, in the middle of a civil war, they did not have the exact data I needed. They did have an idea of where most refugee and displaced persons were located, in encampments, makeshift housing, and hotels along the coast.[5] This information, coupled with some early meetings with representatives of the UN High Commissioner for Refugees, the World Health Organization (WHO), United Nations Children's Fund (UNICEF), and a number of non-governmental organizations (NGOs) involved in supporting the health needs of the refugee and displaced persons, created a map that set me off on a journey around the country to survey these needs in greater depth, establish working relationships and agreements to provide for these needs as a basis for the project.

Years later I would realize that it was in those early days and months that I was learning the basics of project management, learning by doing, or experiential learning as it is called today. I would gain an understanding of the basic concepts of scope, team building, monitoring and control, stakeholder management, and other skills, if not in terms of the definitions and methodologies of project management according to the Project Management Body of Knowledge (PMBOK®),[6] then on an experiential basis. It was later when I earned my Project Management Professional (PMP®) certification that I would more formally internalize this learning.

MANAGING EMERGENCY RESPONSE PROGRAMS IN EASTERN EUROPE AND PREPAREDNESS PROGRAMS FOR NYC AND THE NY/NJ REGION; SHORT LESSONS LEARNED[5]

One of the major lessons learned—practically by accident as a result of not being fully operational until months after the start—was the benefit of starting small and then expanding the project outward. Starting on a smaller scale allows for testing the system, in this case the procurement and delivery mechanism for supplies, before scaling up. This acts as a "proof of concept", so you can figure out what works and, if there are faults in the system, then better to identify those cracks in the system before they are magnified on a larger scale.

There were important considerations that forced this approach; we did not have a good grasp of the needs, had a limited number of staff, and, most importantly, I did not have a good idea of the operating environment, the hazards we might face, or our logistical resource constraints. The assessment of the medical needs, the pipeline for delivery, and logistics requirements would run parallel to that first procurement and delivery.

Three major challenges in this project all had to be balanced against one another: assessing the medical needs of refugees and displaced persons, getting essential medicines and medical supplies to those in need, and tracking those supplies from the warehouse to the end-user. What I practiced then (and what I did not know at the time) is referred to in project management as the "rolling wave approach". This means, like a rolling wave approaching, you prepare based on what you currently know and the relevant immediate near future,

and so I prepared for that first wave of the project, in this instance it was the first three months. So, here is what I knew within the first two weeks:

- In March of 1993, one out of every ten people in Croatia was a refugee/displaced person, with a refugee and displaced person population of over 500,000 people in a country of about 5 million people. There were several large refugee camps in Slavonia (Eastern Croatia, near the Serbian border) and in many of the major hotels along the Dalmatian coast.
- We had a main warehouse in the capital Zagreb and three regional warehouses (Zadar, Split, and Đakovo), plus four small Sport Utility Vehicles (SUVs) (Suzuki Samurai model[7]).
- The project had nine distribution and monitoring staff who were responsible for ensuring delivery and tracking medical supplies to the medical facility (hospital, clinics, etc.), a pharmacist, and a project admin. Many of them had been hired or selected before I arrived.
- We had standing procurement contracts with several international vendors for pharmaceuticals.

Given this situation our initial major objectives (what would now be called an incident action plan [IAP] in emergency management speak) were as follows:

- Establish a logistics system including delivery mechanism, tracking, and reporting, and train staff on this nation-wide and begin the arduous process of explaining the project to healthcare providers and signing assistance agreements. This last item included rules for administering and reporting for pharmaceutical supplies that would be essential for us to verify the paper trail to the end beneficiary.
- Through the Croatian Ministry of Health and UN health coordinating network that included the Red Cross, WHO, Medecins Sans Frontier (MSF; in the US referred to as Doctors Without Borders), and other major relief agencies, assess the most acute public health issues among refugees and displaced persons.
- Identify vendors and initiate a purchase for pharmaceuticals; this necessitated knowing several critical requirements for this procurement:
  - facilities, addresses, and points of contact;
  - types and quantities of pharmaceuticals needed;
  - a waybill system for managing distribution and delivery once the shipment arrived.

This all proved to be much more difficult than anticipated, evident in the troubles we faced with that first shipment. The further breakdown of shipments into smaller deliveries proved much more challenging than anticipated due to poorly marked and packaged pharmaceuticals. Except for pallets, the warehouse lacked the appropriate infrastructure for sorting and repackaging the supplies. Our fleet of Suzuki Samurais proved to be inadequate for the task of delivery, even for the initial small purchase, forcing multiple journeys by our staff, at times through unfamiliar and hazardous roads, to deliver supplies. Uncovering these initial headaches helped to ease the pain with later procurements and smooth our delivery mechanism, allowing us to better focus our limited resources on assessing needs and tracking usage.

While taxing, one effort that proved to be a major success was touring the country for the assessment. Visiting hospitals, health clinics, and refugee medical centers to meet with health professionals, doctors, nurses, dentists, and others to discuss their medical needs helped establish an understanding of the project requirements, and ultimately to develop working relationships with them. A chief outcome of this tour was developing a better situational awareness of the country and a deeper understanding of stakeholder needs and circumstances. This initial needs assessment laid the groundwork for a solid project.

One lesson I learned from those days overseas and the years since then that I carry with me in my project management career is that negotiation is an essential skill for a project manager. Project managers are typically engaging in some type of negotiation at many points in the project lifecycle, if not during the course of a working day. Negotiations take place regularly over resources (staff, equipment, materials, space and systems, IT and communications), schedule deadlines, and the ever-present scope of work and managing—essentially negotiating the project—through inevitable changes. In those early days I would be negotiating to get computer shipments expedited (we only had one 386 laptop when I arrived, mine,[8] which was shared among seven people in my office), for office space, for warehouse space, with client hospitals and health clinics, with our operating local partner, and with our accountants, to name just a few. These were made more complicated by the ongoing civil war, cultural and language barriers, and, quite honestly, my youth.

I was barely 24 years old and managing a large-scale emergency response project at a national level far from home, with little support and guidance, in a country that was not familiar to me (take note International Relations majors; a degree does not confer cultural literacy nor competency). What I lacked in experience, I made up for in perseverance and patience. Listening and focusing in on the needs of your negotiating partner is one of the key ingredients to a successful negotiation, and during those early assessment trips into the field, I did a lot of listening and note-taking, meeting not only with health professionals, but also with leaders in the community and with the community members to hear their stories and understand their circumstances. Once you appreciate where your counterpart is coming from and what you and your partner want to achieve, then it is a matter of finding common ground on which you can both build a mutual understanding through which you can then both accomplish your goals.

However, negotiation is a skill that is a means to balance expectations between competing stakeholders. It is in stakeholder management where gauging stakeholder importance through influences interest, and their involvement in the project helps to grasp the nuances required to balance these needs, be they information, resources, or outcomes. These stakeholders in rank order were as follows:

1. **The funding agency:** The US State Department Bureau for Refugee Programs; without them, funding would not have been available, and there would not have been a project.
2. **The end-recipient (beneficiary):** Identifying and considering their needs was critical since they were the end beneficiaries we were serving.
3. **Client health facilities (hospitals, clinics, etc.)**: They were a critical partner without whom there would be no way to deliver the medical resources we were providing.
4. **Implementing partner (Caritas Croatia and other local humanitarian agencies)**: We had to work with a local partner for HR management, and without their cooperation

and support, we would not have had the facilities or project staff to implement the project.[9]
5. **Project team**: Without the team and their commitment, the project would not have been implemented.
6. **Croatian Government**: Without their authorization to operate in the country, we could not have been operating.
7. **Vendors**: Without them, we would have no supplies and means, warehouses, trucks, etc. to deliver our relief assistance.

This may appear to be obvious, but managing these competing interests was no simple task.

GETTING RELIGION AS A PM – GETTING MY PMP®[3]

Years later when I was in business school, I had the opportunity to study project management as an elective, part of my Master's Degree in the Science of Management.[10] My good fortune was having one of the acclaimed practitioners of project management, Prof. Hans Thamhain,[11] teaching the course. Prof. Thamhain started with the basics of project management and slowly built on those concepts. As he laid out the project management methodology, the experience I had gone through those previous five years started to click into place and make collective sense to me as part of this framework. Scope and stakeholder management, team development, cost estimating techniques and forecasting, and project quality and evaluation methods and tools became starkly evident as part of a larger, extensive, and cohesive framework.

Leveraging those lessons while working as a management consultant a few years later, I used those methods and tools of project management to great effect in my practice. Eventually, I decided to get my PMP® certification from the Project Management Institute®. I prepared for it like anything else, making it a project. Setting the goal was easy: passing the exam and getting my PMP. Of course, there was the application process, which included a listing of all major projects undertaken during your years of experience. Then it was studying, assessing my knowledge, and clocking my time on practice exams, benchmarking my progress along the way to ensure I would walk in and pass the exam, which in 2003 I managed to do.

While some people may find it corny, I keep a copy of the PMBOK® on my shelf close by and hang my PMP® certifications proudly on my wall and, more importantly, take the discipline of project management seriously. As one of my colleagues in project management has said "Project management is a common sense approach to projects, but it requires uncommon discipline" to be effective.[12] What I have learned over my 30+ years as a project manager is that, while seemingly simple, the project management methodology—what is considered to be the better practices as espoused in the PMBOK®—is a powerful approach to getting projects done effectively. I have seen the good, the bad, and the ugly in projects; that latter most often rears up when the simple methods and tools are ignored or paid short shrift, leading to the expected project disaster.

Managing emergencies and emergency plans is no different. The only difference in managing those types of responses to events and project endeavors is that they have higher

stakes, with life and property on the line if a project is mismanaged. It is with this intent that I write this book, as an advisory and, if helpful, a set of guidelines and examples that may help others who are tasked with planning for emergencies (for prevention, mitigation, preparedness, and recovery) and who need to respond to an emergency and think about near term response and long-term plans for recovery.

NOTES

1 The organization was Catholic Relief Services (CRS), a major global humanitarian agency.
2 All names used in this book have been changed to hide identities except where specifically noted or attributed.
3 The project was funded through the US State Department's Bureau for Refugee Programs which would be later renamed the Bureau for Population, Refugees, and Migrants.
4 The term refugee applies to a person who has fled across an international border, from one country to another, while the term displaced person is used for a person who is internally displaced within their own country. Most, if not all, of the refugees who fled into Croatia came from Bosnia-Herzegovina, while the displaced persons came from within Croatia, mostly from areas within or close to the UN Protected Zones (so-called Krajina and Eastern Slavonia).
5 The Croatian coast has been and is once again today a popular tourist destination and filled with hotels that line the rocky banks of the Adriatic Sea.
6 The Project Management Body of Knowledge (PMBOK®) is a recognized set of best practices and published every four years by the Project Management Institute to reflect the current state of practice among leading project management professionals globally. See www.pmi.org for more information.
7 The Suzuki Samurai was not sold in the United States at the time since it was deemed unsafe as it was prone to tipping over; we dubbed them a "tin can with an engine" since they were such a flimsy four-wheel drive vehicle.
8 The one which was assigned to me by my organization.
9 In fact, we were successful in getting the project funded twice more in the years that followed, somewhat unprecedented for what was considered a one-time grant.
10 The MSM at the Arthur D. Little School of Management is now the MBA at the Hult International School of Business located in Cambridge, MA.
11 Prof. Hans J. Thamhain, October 1, 1936 to July 11, 2014 (age 77). He tragically died in a bicycle accident. A memorial page can be found at: www.morrissouthboroughfuneral.com/obituary/Hans-Thamhain
12 Attributed to Stephen Gershenson, a former instructor at the American Management Association.

Chapter 2

Why Project Management Is a Good Fit for Emergency Management

A good majority of work time for most emergency management professionals or managers in public safety, except for those engaged in first response (frontline fire, police, EMS), is engaged in planning and preparation, and a very small percentage of time and effort in response. Those efforts, whether in prevention, mitigation, or preparation, are most often undertaken through projects; projects planned and funded through tax levy dollars or government grant funded programs, and occasionally through public/private initiatives. Let's explore project management in greater depth.

WHAT IS A PROJECT AND PROJECT MANAGEMENT?

While projects and project management have been defined many times in all sorts of publications, they are both more definitively and simply defined in the Project Management Body of Knowledge® (PMBOK). A project as defined in the PMBOK® is "a temporary endeavor undertaken to create a unique product, service, or result".[1] The definition goes on to further elaborate what each of the parameters means, e.g. temporary and unique. In short, a project has a beginning and an end and is designed to create something that has not been done before or is different in some way than what came before. The definition of a project stresses that it is not routine as you might find in operational work, for example manufacturing a product or the delivery of a service on a regular basis. Projects require substantial thinking to tackle the problems that they are designed to solve.

I would further define a project as an undertaking that requires a degree of coordination among a group of people, usually more than three, across functional disciplines (e.g. marketing, finance, and operations). A project is also typically an undertaking that requires more planning and work than a couple of weeks, although I will explain further in this book that an emergency response can be managed as a type of project albeit with a suitable adaptation of the methodology. Indeed, larger emergency responses usually span more than a couple of days, usually weeks after the disaster event has taken place, when it merges into the recovery phase that may take weeks, months, if not years to come to a conclusion.

This leads to the next important definition, and that is *What is project management?* Again, going to the PMBOK®, project management is defined as "the application of

DOI: 10.1201/9781003201557-3

knowledge, skills, tools, and techniques to project activities to meet project requirements".[2] Project management at its core is about managing expectations; managing expectations, first and foremost, of the client, and secondarily, managing the expectations of other key stakeholders: sponsors (who may be clients or internal management), end-users, team members, vendors, etc. At times, those expectations may come into conflict with one another and that requires negotiating between those expectations to bridge the conflicts, from initiating the project to the time it is closed. A skilled project manager is constantly holding those expectations in line while balancing the budget, keeping the project within scope and on time. This is no small feat in normal operating environments, and considerably more challenging in the world of emergency preparedness and response.

DISASTERS, CATASTROPHES, EMERGENCIES, AND EMERGENCY MANAGEMENT

On the heels of defining terms for projects and project management, at this point in the book it is important to define what is meant by emergency management and what prompts the need for emergency mitigation measures and responses. Much like routine or process-based work, there are routine problems or issues that arise in the course of daily work. Typically, these disruptions to daily operations are addressed by individuals or a small team, managed using resources readily available, and are able to restore systems back to their normal state in short order. Examples of these types of incidents are a temporary power outage, minor flooding, or limited fire outbreak.

A disaster, as defined in the Merriam-Webster Dictionary, is "a sudden calamitous event bringing great damage, loss, or destruction".[3] Unlike minor disruptions, a disaster, depending on the severity, usually requires substantial resources (personnel, material, and equipment) that are not normally readily available to be marshaled and deployed to address critical needs in order to restore a system (operations, businesses, etc.) back to its normal order. The effort required by these resources often extends to days, weeks, months, and perhaps even years. More importantly, the distinguishing feature of disasters is that they require a significant level of coordination as they tend to bring together cross-functional and diverse groups of resources, from different organizations, government agencies, volunteers (NGOs, PVOs, CBOs, and FBOs[4]), government agencies, and companies to work together.

Now let's look at what constitutes a catastrophic disaster. While it may seem like an act of semantic interpretation, in the world of emergency management catastrophic disaster events are quite different. A catastrophic disaster is typically one in which the impacts of the disaster exceed the capabilities of the jurisdiction to respond via the collective efforts of all emergency response and recovery agencies that are part of that jurisdictions' emergency plan and/or operations. What also differentiates a catastrophic disaster event is the degree and period for recovery, which is usually extensive. While routine (or lower level) disaster events can be handled locally or within their normal routine, catastrophic damage can take many months, years, and in some cases decades to recover from and includes a wide area of impact and a significant outlay and funds from both public budgets

and private insurers and savings. In some cases previous inhabitants never return and jurisdictions may never fully recover.

A good example of a catastrophic disaster would be the EF5[5] tornado that struck Joplin, Missouri on May 22, 2011; the tornado stretched close to a mile wide and ran a path over 21 miles long and stayed on the ground for close to 20 minutes, destroying over 7,000 homes and numerous municipal buildings, schools, and the main hospital,[6] and killing 160 people.[7] This would be a catastrophe by any stretch of the imagination, but what distinguishes this more than just that was the help needed outside the jurisdiction of the City of Joplin.[8] This help came from neighboring jurisdictions, State and Federal agencies, and major volunteer organizations. Three years following the event, nearly 90% of homes were rebuilt, demonstrating the long period of recovery from such a catastrophe.

An organized response to the critical needs of life-safety, protection and restoration of property, and mitigation of disaster impacts as a result of any major or even catastrophic disaster is carried out through a system of emergency management. Emergency management with its constituent components of planning, prevention, mitigation, preparedness, and response is focused on the coordination of what are called emergency response functions. These emergency functions are broken down into 15 different areas according to FEMA,[9] and these functions are related to life-safety response or, simply stated, preserving human lives and public health: security (law enforcement) and safety (fire service and emergency medical services [EMS]). As referenced above, the secondary missions of any emergency response is to restore property and to mitigate or eliminate the impacts as a result of a disaster. We will explore these further on in this book.

In the sphere of emergency management, this coordinated effort is termed a unity of effort, where these diverse groups work in a coordinated effort toward a common goal. As mentioned in the last chapter, the common working methodology for managing emergencies is called the Incident Command System (ICS), designed to provide a common approach to integrate and coordinate multiple and various resources toward a mutual effort; this system allows the incident command or command element, i.e. the person or people in-charge, to not only effectively direct an emergency response but also to scale up or down the response depending on the situation. While this book is not intended to specifically cover the methodology and terminology of the incident command structure, we will address some of these concepts and techniques as necessary later on in this book in Chapter 15.

The degree to which coordination and management structure necessitates a robust management structure is largely dictated by the size and complexity of the disaster. As outlined in Table 2.1, the National Incident Management System (NIMS) defines the complexity of an incident and the related emergency response along the following parameters.

FEMA defines Incident Complexity Incident and/or event complexity to determine emergency and incident response personnel responsibilities as well as the recommended audience for NIMS curriculum coursework delivery.[10] It is also important to take this incident typology into consideration for emergency planning and preparedness activities, in particular as they relate to the need for project management.

Table 2.1 NIMS Incident Typology

Incident Type	*Incident Description*
Type 1	• This type of incident is the most complex, requiring national resources for safe and effective management and operation. • All command and general staff positions are filled. • Operations personnel often exceed 500 per operational period and total personnel will usually exceed 1,000. • Branches need to be established. • A written incident action plan (IAP) is required for each operational period. • The agency administrator will have briefings and ensure that the complexity analysis and delegation of authority are updated. • Use of resource advisors at the incident base is recommended. • There is a high impact on the local jurisdiction, requiring additional staff for office administrative and support functions.
Type 2	• This type of incident extends beyond the capabilities for local control and is expected to go into multiple operational periods. A Type 2 incident may require the response of resources out of area, including regional and/or national resources, to effectively manage the operations, command, and general staffing. • Most or all of the command and general staff positions are filled. • A written IAP is required for each operational period. • Many of the functional units are needed and staffed. • Operations personnel normally do not exceed 200 per operational period and total incident personnel do not exceed 500 (guidelines only). • The agency administrator is responsible for the incident complexity analysis, agency administration briefings, and the written delegation of authority.
Type 3	• When incident needs exceed capabilities, the appropriate ICS positions should be added to match the complexity of the incident. • Some or all of the command and general staff positions may be activated, as well as division/group supervisor and/or unit leader level positions. • A Type 3 IMT or incident command organization manages initial action incidents with a significant number of resources, an extended attack incident until containment/control is achieved, or an expanding incident until transition to a Type 1 or 2 IMT. • The incident may extend into multiple operational periods. • A written IAP may be required for each operational period.
Type 4	• Command staff and general staff functions are activated only if needed. • Several resources are required to mitigate the incident, including a task force or strike team. • The incident is usually limited to one operational period in the control phase. • The agency administrator may have briefings and ensure the complexity analysis and delegation of authority are updated. • No written IAP is required but a documented operational briefing will be completed for all incoming resources. • The role of the agency administrator includes operational plans including objectives and priorities.
Type 5	• The incident can be handled with one or two single resources with up to six personnel. • Command and general staff positions (other than the incident commander) are not activated. • No written IAP is required. • The incident is contained within the first operational period and often within an hour to a few hours after resources arrive on scene. • Examples include a vehicle fire, an injured person, or a police traffic stop.

PROJECT-BASED WORK AT MANAGING RISK – MITIGATION AND PREPAREDNESS PROGRAMS

Another way of looking at projects, especially in terms of emergency management, is in terms of risk. In brief, a risk on a project is an event that can have a positive or negative impact on the project objectives. Risk in projects is a factor of the investment of time and resources (typically monetized in some way) to yield a positive result. So in a sense, the

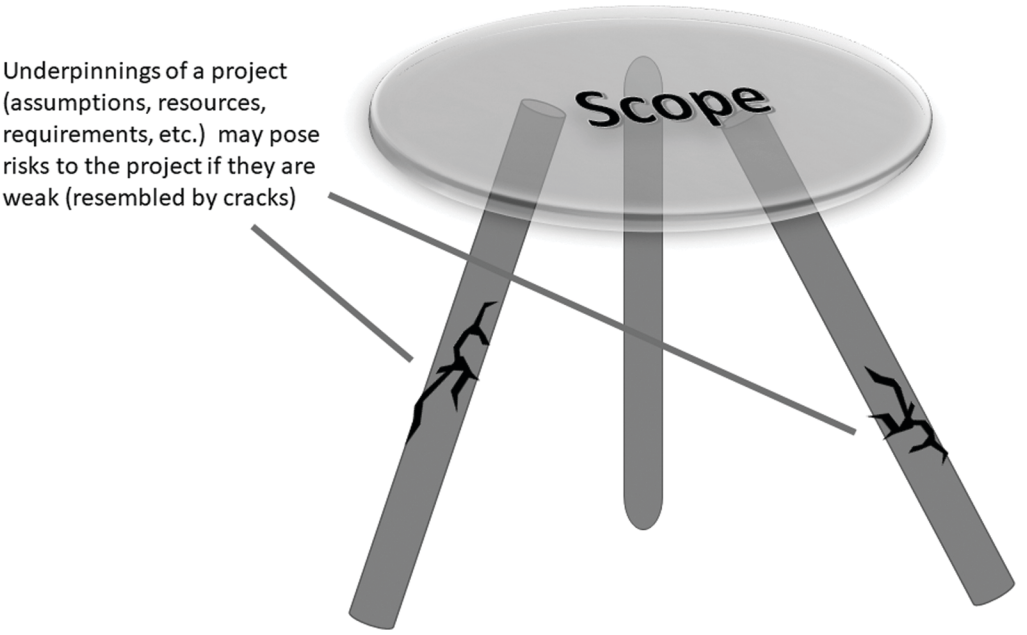


Figure 2.1 Legs supporting a project scope.

organization (whether government, non-profit, or private) is *risking* that investment for what may be deemed a *positive risk* or the benefit gained; the positive outcomes of risk are not always recognized as such although they are certainly present. Unfortunately, risk management is one of the undervalued and under-practiced areas of project management, partly, because many assumptions are taken for granted or important factors are ignored, only to transform into negative risks when the underlying factors that underpin them change, as Figure 2.1 illustrates.

A good example from my own experience was in 1994 when my project was in sore need of an epidemiologist to assess the health status of our client population, and good fortune (a positive risk) brought an epidemiologist from Sarajevo to our doorstep. I had happened to meet her there while I was conducting a short mission to evaluate the needs for an office. She was soon working for our project and solved the niche we needed to fill. I had assumed she would stay with the project for the foreseeable future (that being a year or two). This assumption turned out to be a risk when, after a year in our employ, she informed me that she would be emigrating to Switzerland. We will delve further into risk management in Chapter 3.

While the definition of risk may appear clear to most readers, I have found in my years of consulting and teaching on project-based work that there is some confusion. Again, going to the PMBOK®, a risk can be simply defined as an event that can negatively or positively impact the project in terms of schedule, cost, or scope (the triple constraint). Usually, a risk that primarily impacts one of the constraints winds up affecting the others. Many confuse concerns with risks, such as "the team may not communicate effectively"; this would generally be considered to be a project management quality issue (*note:* not a product quality issue specifically). If, however, the ineffectiveness of team communication

results in the wrong deliverable being sent to the client, e.g. an incorrect design document, then that act (wrong item sent) may be defined as a risk event with associated negative consequences.

Risks in the world of project management are made up of two major components: probability, the likelihood that a risk may occur, and impact on the project, stated initially in monetary terms[11] although there are also schedule impacts (which typically result in monetary impacts). It is through this lens then that risks are identified, defined, prioritized, and managed throughout the lifecycle of the project.

Naturally, the world of emergency management is primarily focused on managing critical risks whether to public safety, health, overall well-being, economy, etc., and proper functioning and the multiple systems that support those ends.

EMERGENCY RESPONSE IS A PROJECT, BEGINNING TO END

All emergency situations, from a low-level disaster to a catastrophic event, have a lifecycle: a beginning and an end. It starts with the trigger of the disaster incident, at times a slow start, such as a storm to those which are sudden, like a tornado, and proceeds through the stages of impact through to recovery. Whether we are looking at those with notice, such as hurricanes, or those with no notice, as in earthquakes, there exists a state of readiness, a response, and recovery to return life to its normal state or what might be called a new normal. In most cases, major or catastrophic disasters leave their mark and change the way of life in the communities they impact.

Much like with a wedding, you can spend months (in some cases years) planning and preparing for the big day or, like some spontaneous couples, get married by a justice of the peace and go to city hall for the marriage license with little ceremony and fanfare. Any efforts prior to or after the event become part of the work. Building levees, instituting earthquake safety standards, creating flood maps, these are all measures taken to mitigate against the damage that natural disasters may cause. Planning, which is the focus of much of emergency management in preparedness, is a complementary component to mitigation and, in some cases, may be looked at as an extension of the mitigation and prevention phase. Once mitigation, prevention, and preparedness measures have been put in place, then any disaster event that arises that requires those emergency responses is put into action. Table 2.2 presents the emergency management process and related projects and examples.

THE ROLE OF THE EMERGENCY MANAGER

Unlike projects in the private sector that are oriented to achieving a return on investment, many projects in the government domain, as well as companies, are aimed at achieving benefits for the public good, clients, customers, or stakeholders which are sometimes difficult to quantify in terms of a return on investment. Emergency mitigation or preparedness projects have been termed “Spending money that governments (and even companies) claim they don’t have on things that they do not want to happen”. The flip side of this is when disasters do strike, then that money and effort is always thought of as having been

Table 2.2 Emergency Management Process and Related Projects and Examples

Phase of EM	*Emergency Management Activity or Project; Examples of Project Types*
Mitigation and prevention	• Building levies to mitigate river flooding • Relocate communities outside of flood zones • Educating the public to increase awareness of household preparedness
Preparedness	• Developing Emergency Operations Plans • Training staff on emergency plans and protocols • Conducting drills and exercises
Response	• Coordinating the evacuation of citizens from flood zones • Deploying search and rescue teams after a devastating earthquake • Building a berm in advance of river flooding
Recovery	• Debris removal after a tornado • Restoring power after a major power outage • Rebuilding a community after a natural disaster

well spent or is assumed to have been present, when in fact it took years of work, justification, and planning and exercises to pull off a successful response.

In this paradox that elected leaders and government officials find themselves, they are managing the tension as stewards of taxpaying dollars (or other currencies outside the United States) and balancing this against preparing for the response to the exigencies of disasters. Government leaders are accountable to the budgeting process, fiscal reporting, interest and "watchdog" groups, the press, and finally government audit. Most support for long-term emergency mitigation and preparedness programs is funded at the Federal level through grants to the states which distributes this funding and manages it down to the local level, either on a county or municipal level. This cycle takes years, often with grant funded projects and programs being carried out over the same time frame, at times with seemingly unrealistic deadlines when approvals run late and/or get mired in legal contracting between emergency agencies and vendors.

Many emergency managers have risen through the ranks, from the field level, as an EMT, firefighter, or police officer through the ranks to a captain, chief, or senior leader in their organization. Most of the work that these middle and line managers in first response (law enforcement, the fire service, and emergency medical service) is operational response: responding to an emergency call, debriefing and reporting on these calls, training to improve their capabilities, and daily administration, maintenance, and support for these operations.

New projects, such as creating new public safety programs, adopting new methods, techniques, or technologies, developing an exercise, require aspects of project management: managing project scope, timelines, and budget, which may not be familiar skills for many of these managers and leaders, so the guidance in this book is intended to add to their toolkit. As many colleagues in the field have related to me, the greater percentage of work a professional emergency manager is engaged in on a regular basis is project based, and a much smaller percentage in response (with the exception of the pandemic).

Additionally, in major disaster responses, when managing different functional responses, emergency managers, whether operating within a Unified Command or Single Command in cooperation, are working cross-functionally, marshaling limited resources toward a common goal within operational periods and interim objectives, but with an unclear

initial scope and undefined end date and exit strategy; all aspects of project management, albeit best described as "rolling wave project management".

In the United States, emergency management in response to larger events, with multiple operational periods and multi-agency response, has largely been governed by the Incident Command System (ICS) since its adoption as a methodology in the 1970s and development in the ensuing decades, incorporated as part of the National Incident Management Systems (NIMS).[12] While ICS does address the needs of managing multi-agency, public, and private organizational coordination for large complex emergency events, there is a need to fill gaps when it comes to understanding and managing the scope of new projects (training, adopting new technology such as ICS software, or the larger management of drills and exercises); and managing human resources, budgets, schedule, procurement, quality, communication, and risks related to project management (not the usual operational risks). The full spectrum of project management methods addresses these needs through an integrated approach to these managerial activities.

A couple of items I want to note before the moving on to rest of the book. While this book is intended to explain the connection between project and emergency management and provide a solid context, it is not intended to cover these two subject areas, or the related areas of risk management or leadership, in exhaustive depth. There are numerous books and standards that delve into these areas, some of which I reference in this book. Although most of the references, frameworks, and methodologies are based on US models, one of my objectives of the book is to target a global audience. I have referenced frameworks used in other parts of the world, ISO, UN, etc., so no matter where you may be based on the globe, professionals in emergency management and public safety will be able to understand and apply these concepts and methods in their own context. Lastly, some concepts may appear to be only relevant to one audience, so I may at some points in this book answer the question as to "why this is important", explaining the relationship of a concept or method to the current state of common practice.

NOTES

1 *Project Management Body of Knowledge, 3rd Edition*, 2004 Project Management Institute, Four Campus Boulevard, Newtown Square, PA, p.5.
2 *Project Management Body of Knowledge, 3rd Edition*, 2004 Project Management Institute, Four Campus Boulevard, Newtown Square, PA, p.8.
3 From Merriam-Webster: www.merriam-webster.com/dictionary/disaster?utm_campaign=sd&utm_medium=serp&utm_source=jsonld
4 NGO=Non-Governmental Organization, PVO=Private Voluntary Organization, CBO=Community-Based Organization, FBO=Faith-Based Organization. Each of these terms describes a type of organization that comprises both paid and volunteer staff; NGO is typically used internationally and describes humanitarian relief, response, and development organizations with paid staff.
5 EF stands for Enhanced F Scale for Tornado damage. This rating scale is similar to the Saffir-Simpson scale for hurricanes in that the skills are based on ranges of wind gust estimates based on an evaluation of damage, usually taken immediately after a tornado event. The F scale was originally developed by T. Theodore Fujita of the University of Chicago in 1971. This was subsequently updated in 2007. Reference: www.spc.noaa.gov/faq/tornado/ef-sclae.html

6 NCDC Event Record. NCDC Storm Events Database. National Oceanic and Atmosphere Administration, National Climatic Data Center. See www.ncdc.noaa.gov/stormevents/eventdetails.jsp?id=296617
7 McCune, Greg (November 12, 2011). "Joplin tornado death toll revised down to 161". Reuters. See www.reuters.com/article/us-tornado-joplin/joplin-tornado-death-toll-revised-down-to-161-idUSTRE7AB0J820111112
8 Powerful tornadoes kill at least 31 in US Midwest. Kevin Murphy (Reuters) May 22, 2011. See www.reuters.com/article/us-usa-weather-tornadoes/tornado-devastates-joplin-missouri-116-dead-idUSTRE74M08L20110523
9 www.fema.gov/media-library/assets/documents/25512
10 National Incident Management System Incident Complexity Guide: Planning, Preparedness and Training (fema.gov). See www.fema.gov/sites/default/files/documents/nims-incident-complexity-guide.pdf
11 As we will get into later in Chapter 4, the monetary term used is the expected monetary value (EMV).
12 Gil Jamieson (2005) NIMS and the Incident Command System. International Oil Spill Conference Proceedings: May 2005, Vol. 2005.

SECURITY, AUDIT AND LEADERSHIP SERIES

Ulf Mattsson

VOLUME II

Controlling Privacy and the Use of Data Assets

What is the New World Currency—Data or Trust?

CRC Press
Taylor & Francis Group

Praise for the Book

"Ulf's experiences are applied pragmatically to where the world is today and headed in the future. The methods and systems described in the book will help any group accelerate improves and maintain data and privacy practices."

—Brian Albertson, CRISC, CDPSE, ITIL, VP of Operations for ISACA Atlanta Chapter, IT Risk Management Execution Led, State Farm

"Ulf Mattssons's book will help distill the complexities of privacy into a concise, compact, easy-to-follow desktop reference. As privacy becomes more important to a company's operational well-being and survival, with GDPR and other privacy-related fines heading upwards to the millions and sometimes billions of dollars, security leaders, especially in small and midsized firms, are finding their swim lanes getting broader, encompassing privacy as an area of responsibility. This book will help navigate, identify gaps and provide practical examples and ideas for building a sustainable and essential privacy framework for any organization."

—Wei Tschang, CISSP, CIPP/US, CISA, CISM, CGEIT, First VP for ISACA New York Metropolitan Chapter, Head of Information Security, Cadwalader, Wickersham, & Taft LLP

"Ulf Mattson, whose security insights I have cherished for years, has written the book that C-levels need to read. Data's value to an enterprise is well known, but Ulf explores how it's also a danger. It's a danger to the business in the hands of a cyberthief, it's a danger to the business if it disappears (accidentally or maliciously), it's a danger to business operations if it can't be effectively managed, analyzed, stored and retrieved and it's absolutely a danger to an enterprise when it hurts customers, which is what new data privacy laws are all about. Is data friend or foe? Frustratingly, it's both. Read this book to know how to control data and stop it from controlling you."

—Evan Schuman, Computerworld weekly columnist, Moderator for MIT Sloan Management Review events, Member, Internet Press Guild

"Information and its usage is a massive component of the digital economy, something Ulf discusses extensively in this book. For privacy professionals looking to understand the complexities of applications at scale in this age, this book provides excellent (if not terrifying) diagrams of how modern systems work. APIs and distributed systems create value together, but that creates unique problems for those of us tasked with protecting the data driving that value. For cybersecurity professionals who want to understand more of what risk and privacy leaders are looking to solve for, this book provides crucial insight into the minds of privacy professionals as they work to apply legal and regulatory frameworks to daily operations."

—Branden R. Williams, DBA, CISSP, CISM

Controlling Privacy and the Use of Data Assets

The book will review how new and old privacy-preserving techniques can provide practical protection for data in transit, use, and rest. We will position techniques like Data Integrity and Ledger and will provide practical lessons in Data Integrity, Trust, and data's business utility.

Based on a good understanding of new and old technologies, emerging trends, and a broad experience from many projects in this domain, this book will provide a unique context about the WHY (requirements and drivers), WHAT (what to do), and HOW (how to implement), as well as reviewing the current state and major forces representing challenges or driving change, what you should be trying to achieve and how you can do it, including discussions of different options. We will also discuss WHERE (in systems) and WHEN (roadmap). Unlike other general or academic texts, this book is being written to offer practical general advice, outline actionable strategies, and include templates for immediate use. It contains diagrams needed to describe the topics and Use Cases and presents current real-world issues and technological mitigation strategies. The inclusion of the risks to both owners and custodians provides a strong case for why people should care.

This book reflects the perspective of a Chief Technology Officer (CTO) and Chief Security Strategist (CSS). The Author has worked in and with startups and some of the largest organizations in the world, and this book is intended for board members, senior decision-makers, and global government policy officials—CISOs, CSOs, CPOs, CTOs, auditors, consultants, investors, and other people interested in data privacy and security. The Author also embeds a business perspective, answering the question of why this an important topic for the board, audit committee, and senior management regarding achieving business objectives, strategies, and goals and applying the risk appetite and tolerance.

The focus is on Technical Visionary Leaders, including CTO, Chief Data Officer, Chief Privacy Officer, EVP/SVP/VP of Technology, Analytics, Data Architect, Chief Information Officer, EVP/SVP/VP of I.T., Chief Information Security Officer (CISO), Chief Risk Officer, Chief Compliance Officer, Chief Security Officer (CSO), EVP/SVP/VP of Security, Risk Compliance, and Governance. It can also be interesting reading for privacy regulators, especially those in developed nations with specialist privacy oversight agencies (government departments) across their jurisdictions (e.g., federal and state levels).

First edition published 2024
by CRC Press
2385 Executive Center Drive, Suite 320, Boca Raton, FL 33431

and by CRC Press
4 Park Square, Milton Park, Abingdon, Oxon, OX14 4RN

CRC Press is an imprint of Taylor & Francis Group, LLC

Library of Congress Cataloging-in-Publication Data
Names: Mattsson, Ulf, author.
Title: Controlling privacy and the use of data assets : what is the new world currency - data or trust? / Ulf Mattsson.
Description: First edition. | Boca Raton : CRC Press, 2024. | Series: Security, audit and leadership series | Includes bibliographical references.
Identifiers: LCCN 2023007091 (print) | LCCN 2023007092 (ebook) | ISBN 9781032185163 (hardback) | ISBN 9781032185187 (paperback) | ISBN 9781003254928 (ebook)
Subjects: LCSH: Data privacy. | Data protection.
Classification: LCC HD30.3815 .M37 2024 (print) | LCC HD30.3815 (ebook) | DDC 323.44/8--dc23/eng/20230510
LC record available at https://lccn.loc.gov/2023007091
LC ebook record available at https://lccn.loc.gov/2023007092

ISBN: 978-1-032-18516-3 (hbk)
ISBN: 978-1-032-18518-7 (pbk)
ISBN: 978-1-003-25492-8 (ebk)

DOI: 10.1201/9781003254928

Typeset in Times
by SPi Technologies India Pvt Ltd (Straive)

Contents

SECTION II Trust and Hybrid Cloud

SECTION III Data Quality

Foreword – Ben Rothke, CISSP, CISM, Senior Information Security Manager, Tapad, Inc. New York, NY

I've read countless security books over the last 20 years. After reading tens of thousands of pages of security and privacy text, I think I found what it takes for an excellent information security book. It is the combination of a relevant topic, a knowledgeable author, who is also a capable writer. Some of the books I've read have none of those, many have two, and only a few have all three.

I've known Ulf Mattsson for many years, and he has consistently been able to write excellent content. With a master's degree in physics, he knows that the micro level can significantly impact a system. And with his broad real-world experience at some of the world's largest and most sophisticated companies, he knows what it takes for things to work at the system level.

In 2023, the amount of data seems to expand more quickly than the universe. An average midsize company has more data than those that exist in the Library of Congress. With that much data, firms today deal with multiple competing needs and tensions around their data. Issues, such as access vs. availability, siloed vs. open, and more, require Chief Information Security Officers (CISO) to make decisions that affect all of the data, the liquid gold of the organization.

If they take too aggressive of an approach to data access, overall corporate efficacy can suffer. Too open access to the data, and the company will be on the receiving end of a class action lawsuit. Being able to balance those competing needs requires the steadiness of a tightrope walker.

Most CISOs have to deal with the same tension as tightrope walkers do. And what every tightrope walker has is a pole. They carry these poles during a performance to maintain stability while walking on a narrow rope. It also lowers the center of gravity of the tightrope walker, giving them a greater level of stability.

Ulf has written a book that can be used as a tightrope walker pole for a CISO or anyone tasked with information security management. Terms such as trust, security, privacy, zero-trust, and more are bandied about, often with little guidance on implementing them. Ulf gives the reader everything they need to know to balance the many competing things around data access.

When it comes to security and privacy, the devil is in the details. And this book is heavy on those details. As the details are all the difference between legitimate access and an attacker pilfering the data. For those serious about the topic, this is a broad and deep book written by an author with significant depth and breadth.

The role of a CISO today is to ensure that the CEO's picture is not in the Wall Street Journal due to a data breach. And Ulf's book will help you understand what you have to do in order to do that.

Foreword – Jim Ambrosini, CISA, CRISC, CISSP Cybersecurity Consultant and CISO

"Data is the new oil"—or so we've been told.

For the past 20 years, data has been the key to competitive advantage. Companies that use it effectively have reaped the benefits. This notion has given rise to entire industries and educational programs geared toward the manipulation, analysis, and presentation of data. "BI" or "Business Intelligence" was what we used to call it. Now it's "Data Mining" or "Big Data"—terms that seem more appropriate. But we've hit a bump in the road. Data is only as good as the trust we place in it. How do we trust data in a world with escalating breaches—where it's not a question of "if" a company will get breached, but "when"? As a CISO for several corporations, this is top of mind for me, as well as my clients.

Hence, the new currency—Trust. Data that can be trusted is a prerequisite in all decision-making and transaction processing. The concept of complete trust in data is somewhat of a mythical unicorn—no data can be 100% secure and trusted, right? Or can it?

This is the focus of Ulf Mattson's new book. Volume 1 discussed different forms of access controls and methods to safeguard data. His new book takes the reader through the journey toward Zero Trust. Zero Trust is an IT security model that requires every user and connected device to verify their identity prior to accessing the data. By enforcing Zero Trust architecture, you, essentially, trust no one or no device—until proven otherwise. In this way, you are imbuing trust in the data by ensuring only authorized people or devices have access to it. And yes, it is a journey, not an end state.

I see far too often companies implementing the latest technology or tool promoting "Zero Trust"—but it's not that simple. One of the things I like about this book was how Ulf describes the Zero Trust maturity model as well as tactics for Cloud migrations and network access. He's essentially laid out the roadmap for us. The book flips the script from "Trust and Verify" to "Verify then Trust".

I should spend a minute speaking about the author, Ulf Manson. I came to know Ulf around 2011. I was the President of the ISACA Chapter of New York (ISACA is the largest organization of information security, risk, and audit professionals in the world). The New York Chapter would put on various educational events and conferences, as we were always looking for qualified speakers. Someone recommended Ulf to speak about Data Security—and after that first time, I had him back regularly. Honestly, after each session, I would ask myself "How does this guy know so much about this topic?" I realized the answer—he lives it.

During his career, ULF has been a Chief Security Strategist, Chief Technology Officer, and the founder of Protegrity—a company that specializes in data security. He is also a frequent public speaker on the topic of data trust at numerous conferences and events.

It's fortunate for most of us that Ulf can translate complex technical details into bite-size chunks that are easily understandable. This book is no different and does not disappoint.

I see this book as a reference guide for system engineers, network administrators, consultants, and CISOs. In fact, I am using it right now to dialogue a strategic data security program for one of my clients. It's going to resource that will be referred to for a long time. Zero Trust is the new gold. This book is the treasure map.

Foreword – Richard Purcell, CEO, Corporate Privacy Group (former Chief Privacy Officer, Microsoft)

In his first volume of *Controlling Privacy and the Use of Data Assets*, Ulf Mattsson described the world's achievement of a technologically significant moment—a world in which data is the "new oil", providing the driving force for economic and social development. He described a number of practices, processes and tools which, when properly and carefully applied, amplify data's accelerant power.

In this succeeding volume, Ulf tackles the logical next question—if data is the driving force, then what is the currency of exchange? As a resource, data is indisputably the foundational element of modern progress, but what is the mechanism for managing the resource? Is it the transportation processes themselves, the data lifecycle of collecting, processing, storing, distributing, and managing the resource? Or is it the confidence that those processes are transparent, fair, reasonable, and designed for broad benefit? In other words, in a world that accepts the dominance of a singular resource, what do we want as the controlling factors that assure its utility to more than the "many chosen few"?

An analogy comes to mind, one that has been decades in the making. The development and application of safety practices for hazardous materials has provided economic, social, and personal benefits through standardized classifications, markings, handling procedures, emergency response measures, storage protocols, and disposal requirements. The next time you see a tanker trailer next to you on the road, look for the placard showing what material and level of handling is on board.

So, why is it, after several decades of information technology, data creation and use, and security breach reporting, that we have not yet undertaken the job of developing similar standards of care for the collection, use, storage, sharing and management of personal data? We have volumes of experience across the globe from engineers, scientists, transportation experts, and others who collaborated with legislative assemblies to develop and promulgate standards to protect the public and private interests in manufacturing, storing, transporting, and disposing of hazardous materials. They have done the heavy lifting already by creating a framework useful for such an undertaking.

In this and his first volume, Ulf Mattsson points the way toward how such an effort could begin to take shape through an understanding and categorization of data types and environments as well as best practices for providing safety protocols to prevent intentional or accidental corruption of the safeguards.

In an age in which Artificial Intelligence and Synthetic Media are quickly becoming the fundamental underpinnings of products and services, such protections are more urgently needed than ever before. Such standards, including the ethical approaches to research, design, development, and deployment of these products and services could mitigate the underlying questions of trust they inherently present. There should never be any doubt in the consumer marketplace as to reality that is experienced or distorted. Our marketplace confidence depends on knowing the distinction; we enjoy fictions today because we know they are fictions and meant to entertain, challenge, and/or stimulate. When those fictional narratives become attempts to distort, though, we have not just a problem but a weakening of our social and economic foundations—disaster lurks.

There is no easy route to global standards, we know. And that is no reason to not take Mr. Mattsson's thoughtful guidance to heart as a good starting point to work the problem. Many have come before us and mapped out the process. Ulf and others are complementing their work by providing us comprehensive and smart inputs to the content—the currency of trust in a data-driven world.

About the Author

Ulf Mattsson is a recognized information security and data privacy expert with a strong track record of more than two decades implementing cost-effective data security and privacy controls for global Fortune 500 institutions, including Citigroup, Goldman Sachs, GE Capital, BNY Mellon, AIG, Visa USA, Mastercard Worldwide, American Express, The Coca Cola Company, Wal-Mart, BestBuy, KOHL's, Microsoft, IBM, Informix, Sybase, Teradata, and RSA Security. He is currently the Chief Security Strategist and earlier the Chief Technology Officer at Protegrity, a data security company he co-founded after working 20 years at IBM in software development. Ulf is an inventor of more than 70 issued U.S. patents in data privacy and security.

Ulf is active in the information security industry as a contributor to the development of data privacy and security standards in the Payment Card Industry Data Security Standard (PCI DSS) and American National Standards Institute (ANSI) X9 for the financial industry. He is on the advisory board of directors at PACE University, NY, in the area of cloud security and a frequent speaker at various international events and conferences, including the RSA Conference, and the author of more than 100 in-depth professional articles and papers on data privacy and security, including IBM Journals, IEEE Xplore, ISSA Journal, and ISACA Journal.

Ulf holds a master's in physics in Engineering from Chalmers University of Technology in Sweden.

Introduction

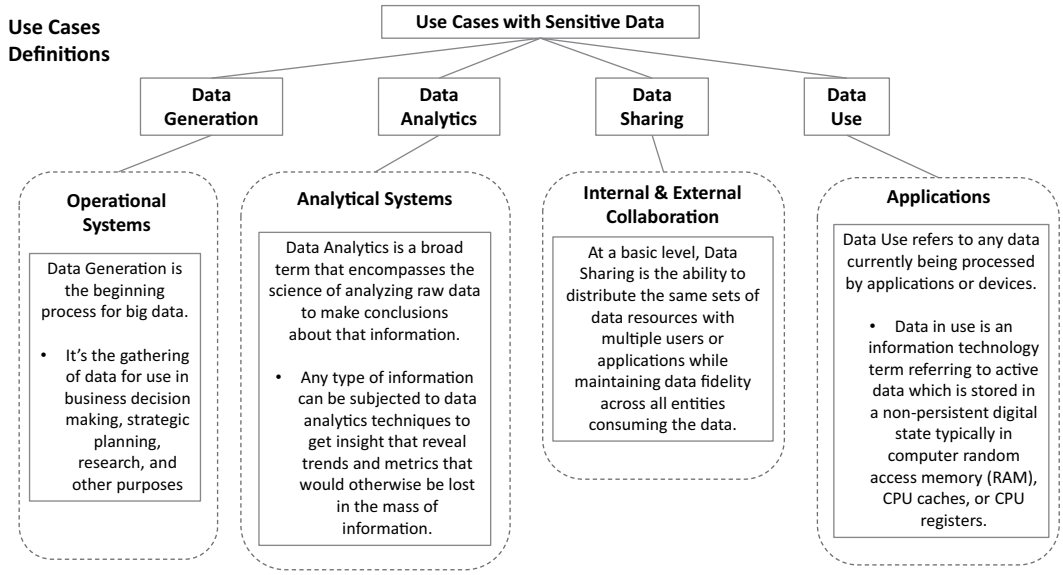
Thank you for taking the time to read my book about protecting your data. This book is about Data Integrity and Trust in Data.

The book will review how new and old privacy-preserving techniques can provide practical protection for data in transit, use, and rest. We will position techniques like Data Integrity and Ledger.

Why do we need this book?

This book will use practical lessons in Data Integrity, and Trust, and data's business utility.

This book is based on a good understanding and experience of new and old technologies, emerging trends, and a broad experience from many projects in this domain. This book will provide unique context about the WHY (requirements and drivers), WHAT (what to do), and HOW (how to implement), and review current state and major forces representing challenges or driving change, what you should be trying to achieve, how do you do it, including discussions of different options. We will also discuss WHERE (in systems) and WHEN (roadmap). Unlike other general or academic texts, this book is being written to offer practical general advice, outline actionable strategies, and include templates for immediate use. The book contains diagrams needed to describe the topics and Use Cases, for example.



WHO SHOULD READ THIS BOOK?

The book presents current real-world issues and technological mitigation strategies. The inclusions of the risks to both owners and custodians provide a strong case for why people should care.

The book reflects the perspective of a CTO and Chief Security Strategist. I worked in and with startups and some of the largest organizations in the world. The book is for board members, senior decision-makers, and global government policy officials—CISOs, CSOs, CPOs, CTOs, auditors, consultants, investors, and other people interested in data privacy and security. I will also embed a business perspective. Why is this an important topic for the board, audit committee, and senior management regarding achieving business objectives, strategies, and goals and applying the risk appetite and tolerance?

The focus is on Technical Visionary Leaders, including Chief Technology Officer, Chief Data Officer, Chief Privacy Officer, EVP/SVP/VP of Technology, Analytics, Data Architect, Chief Information Officer, EVP/SVP/VP of I.T., Chief Information Security Officer (CISO), Chief Risk Officer, Chief Compliance Officer, Chief Security Officer (CSO), EVP/SVP/VP of Security, Risk Compliance, Governance.

It can also be interesting reading for privacy regulators, especially those in developed nations with specialist privacy oversight agencies (government departments) across their jurisdictions (e.g., federal and state levels).

WHY IS VOLUME 2 OF THIS BOOK NEEDED?

The reader may be interested in different aspects of data privacy and security landscape. This book is discussing perspectives. For example:

- "Trust the User, App, and Data" and how technologies and regulations can address these issues. And the right balance to be found with technologies that can strongly enforce rules and regulations
- Ransomware and other malware are taking different forms of attacking your systems and data
- A roadmap that is addressing different issues
- ABAC (attribute-based access control) or PBAC (policy-based access control) and the journey into zero trust
- Planning for Web 3.0 that can address data ownership
- Planning for issues and benefits of quantum computing
- Synthetic data that can be generated in different ways and measured in terms of risk and utility levels
- Collecting more context in finding privacy issues by evolving ways of scanning applications and implementing privacy by design
- Applying the techniques for different use cases in cloud and increasingly distributed environments that is used by an increasingly distributed workforce
- When to apply these from various data types of different types and different use cases
- Staffing of departments working on privacy and security for different maturity and size of organizations
- Spending on privacy and security across different industries
- Prioritization and alignment of various industry standards and guidance for different regions
- Different types of product vendors that are focusing on various aspects of data privacy and security
- Prescriptive to different use cases and each industry
- You cannot manage what can't measure. Metrics are important for example Zero Trust maturity

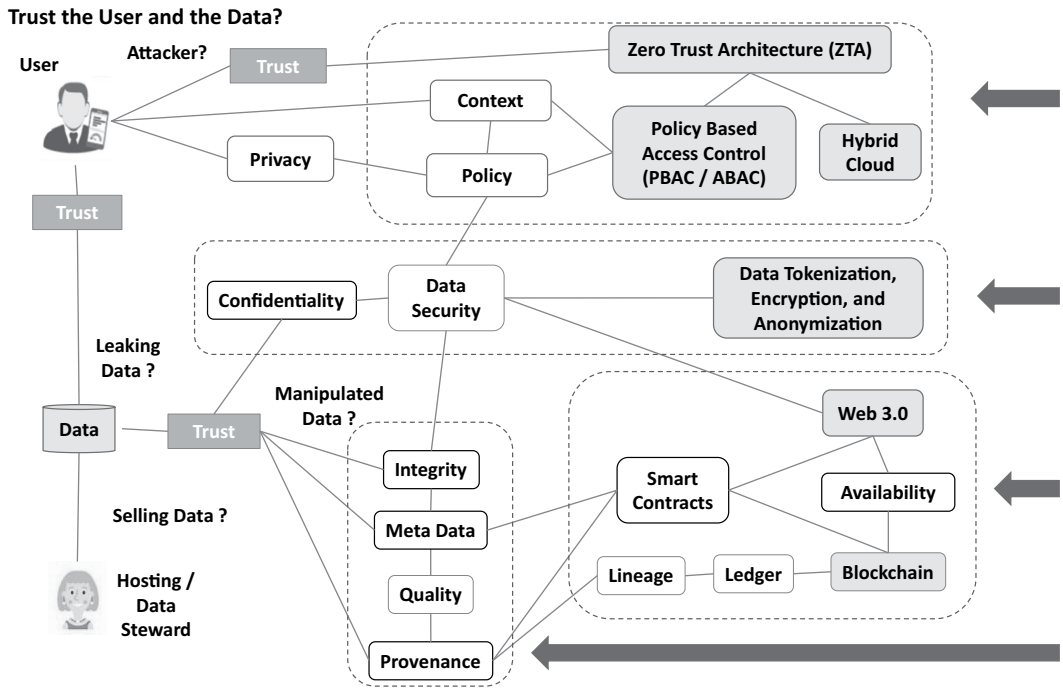
HOW TO READ THE BOOK

The Introduction provides a high-level overview, and more technical aspects are discussed in different chapters.

Discussions about Trust in User, Apps, and Data

Privacy and security issues and solutions related to User, App, and Data can be found in the different chapters. The Zero Trust chapter (5) discusses users and authorization. Data Quality and Integrity is

discussed in separate chapters (8 and 9). Web 3.0 is discussed in Chapter 7. User access is discussed in the ZTA chapter and data confidentiality and integrity aspects are discussed in other chapters: We will focus on the user, data security, web security, and data quality:



THE FUTURE OF DATA PRIVACY TECHNOLOGIES

This book will discuss how the landscape of data privacy and security is evolving and an online version with different appendices will keep the information up to date:

New risks		
Evolving ransomware and other threats to data	New data privacy regulations	Evolving work force with new work environments
Evolving technologies		

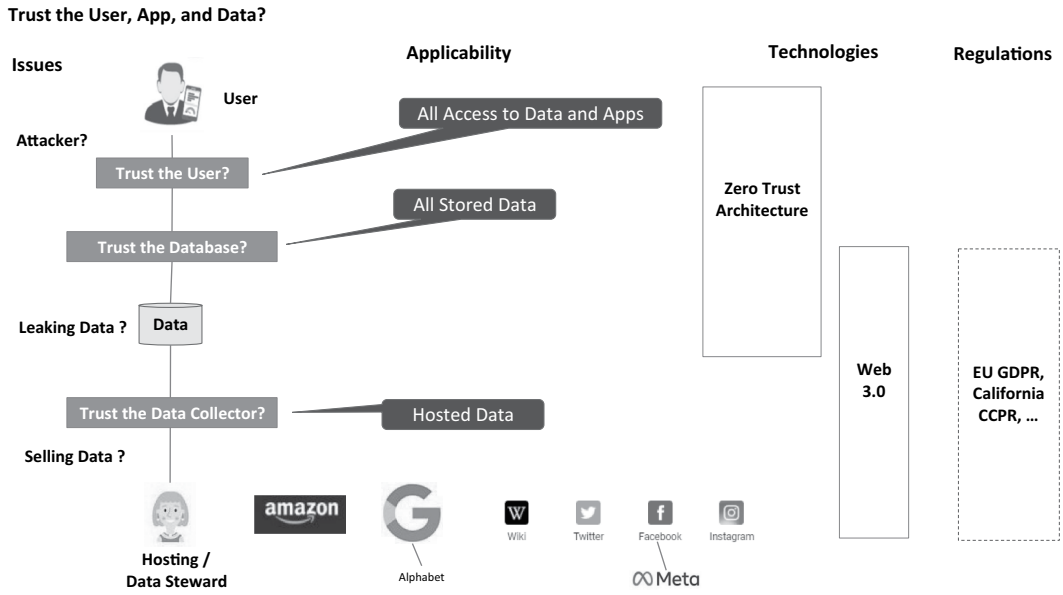
The first book, "Volume I", focused on basic platforms and data protection techniques and a shorter introduction to evolving platforms and data protection techniques.

The theme in this book, "Volume II", is about "The Future of Data Privacy" and talks more about evolving platforms and data protection techniques. A few of the chapters address "Who Owns the New Oil?" and talks about technologies that can help in owning and controlling your private data. It is hard to predict the future but I'm discussing some important technologies that can have great impact.

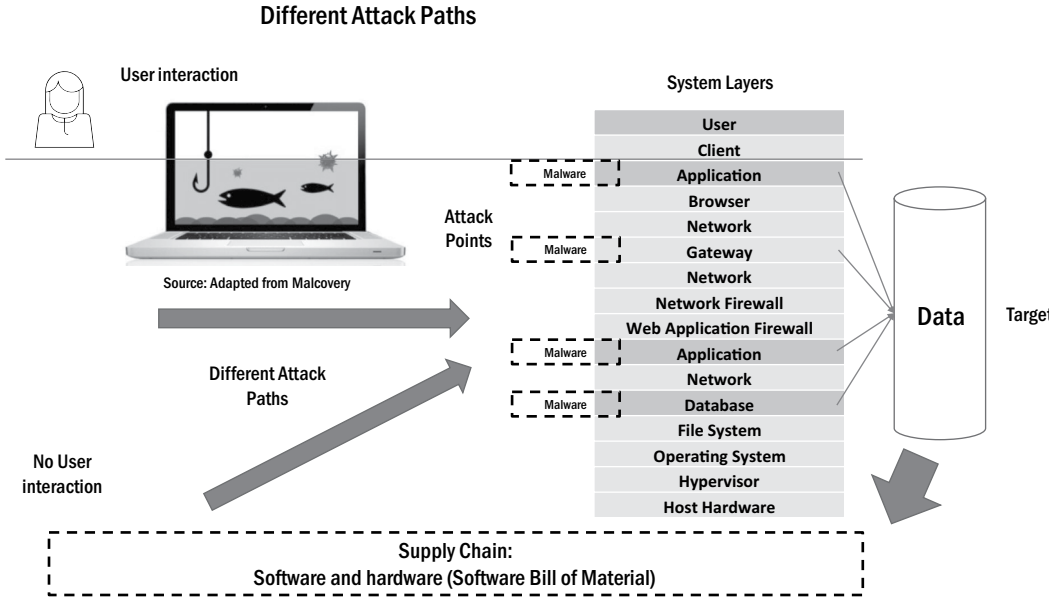
Additional appendices can be found in the online section. This allows for timely updates.

The different chapters talk about the issues of "Trust the User, App, and Data" and how technologies and regulations can address these issues. The user may not be the real user. Data may be attacked and leaked from data storage. Some hosting is collecting and selling your private data. Different technologies can address the issues of user access and data leakage. Other technologies

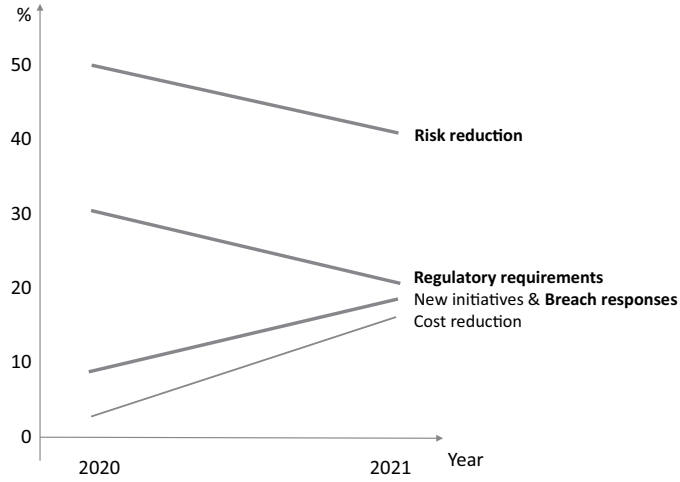
can address data ownership and issues of data sharing. The right balance could be found with technologies that can strongly enforce rules and regulations may not be strongly enforced:



Ransomware and other malware are taking different forms of attacking your systems and data. Education is important, but technology is needed to continuously defend against these attacks. We will discuss how zero trust can create a new perimeter around your critical resources. Attackers may already be in your system and Chapter 1 is discussing that attacks are coming from different directions and how a layered security model can catch attackers at different layers:



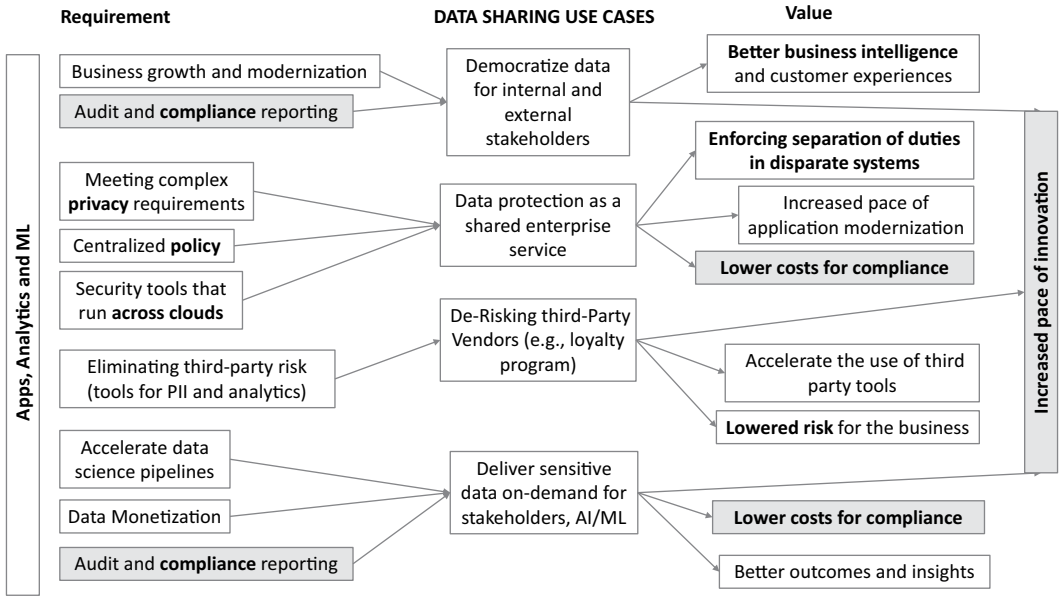
These are drivers for cybersecurity spending according to EY. Top drivers are still risk reduction and regulatory compliance. New initiatives, breach responses, and cost reduction are on the rise:



Source: Adapted from EY

REQUIREMENTS, USE CASES, AND BUSINESS VALUES

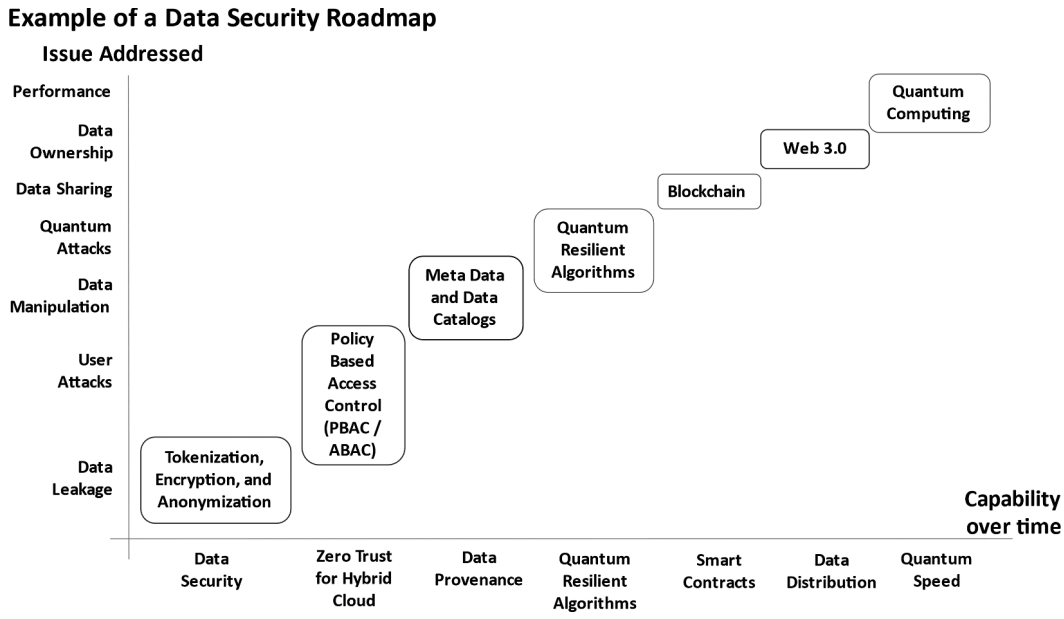
We will discuss different requirements, use cases, and business values in this book. EY reported that top drivers are still risk reduction, innovation, lower risk, and breach prevention and lower cost for compliance are on the rise. We will review some data sharing use cases with the top requirements and values that also focus on centralized data privacy policy across hybrid cloud, analytics, and ML:



We will discuss some DATA SHARING solutions that enable these data privacy capabilities:

- Anonymization SDKs for Cloud and on-prem.
- Generative AI for Test Data Management with Synthetic data generation.
- Generative AI for AI/ML with Synthetic data generation.
- Data Sharing Patterns and guidance for safely sharing data.

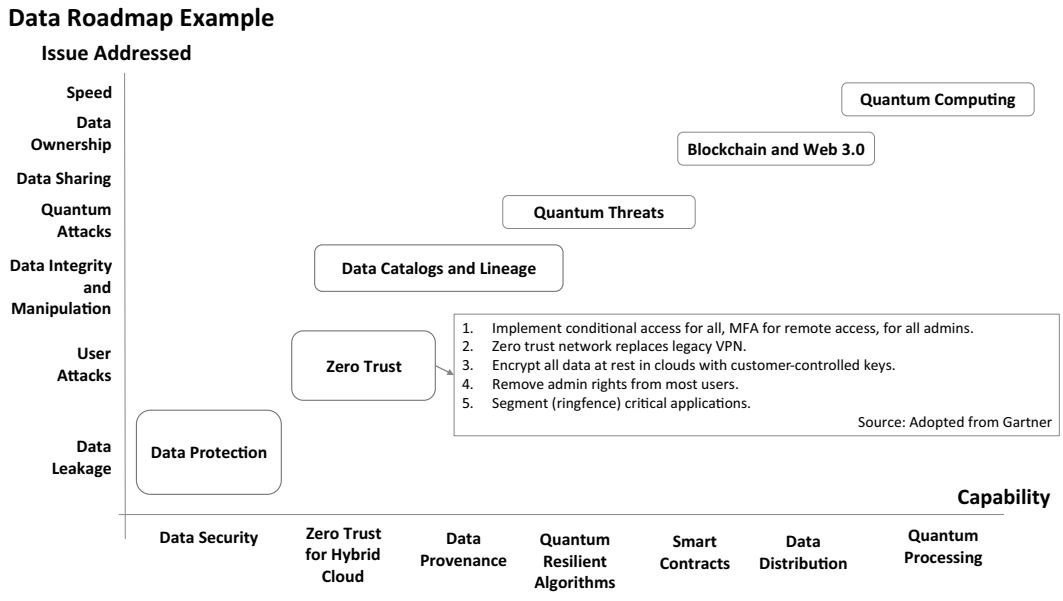
Interest in different solutions and capabilities can be another way to enter the book. A roadmap that is implementing Zero Trust and addressing the discussed issues is outlined in Chapter 3:



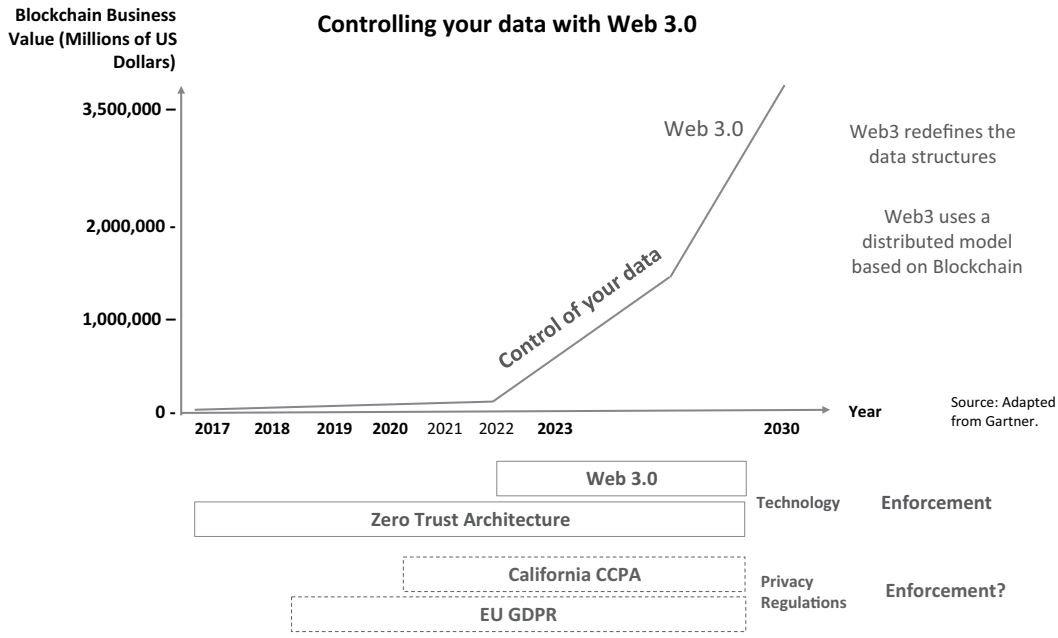
Discussions about System Capabilities

Different chapters are discussing capabilities to address the different issues. The capabilities may also be laid out over time when different issues may be addressed.

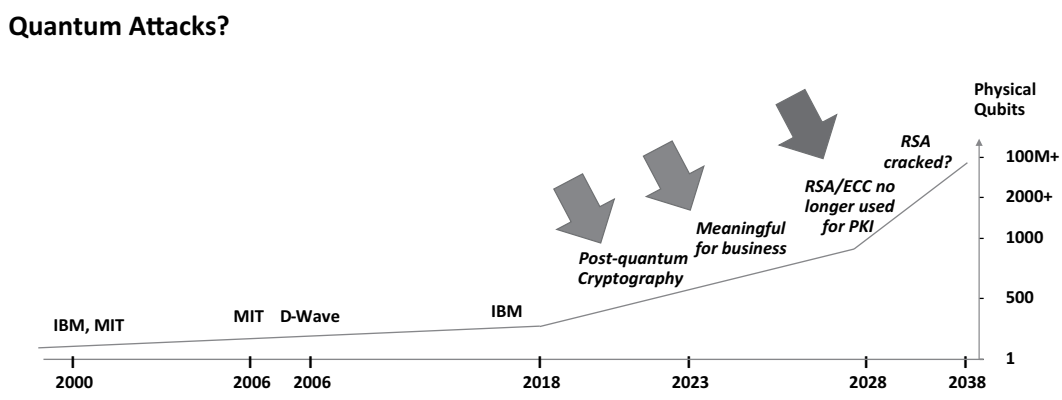
Volume I discussed different forms of access control, including "dynamic authorization to resources" including ABAC (attribute-based access control) or PBAC (policy-based access control). This book will discuss the jouney into zero trust that can address several of the issues. We discuss the small steps that can be taken by implementing multifactor authentication and policy-based and dynamic authorization to resources:



Planning for Web 3.0 can address data ownership is discussed in Chapter 3:

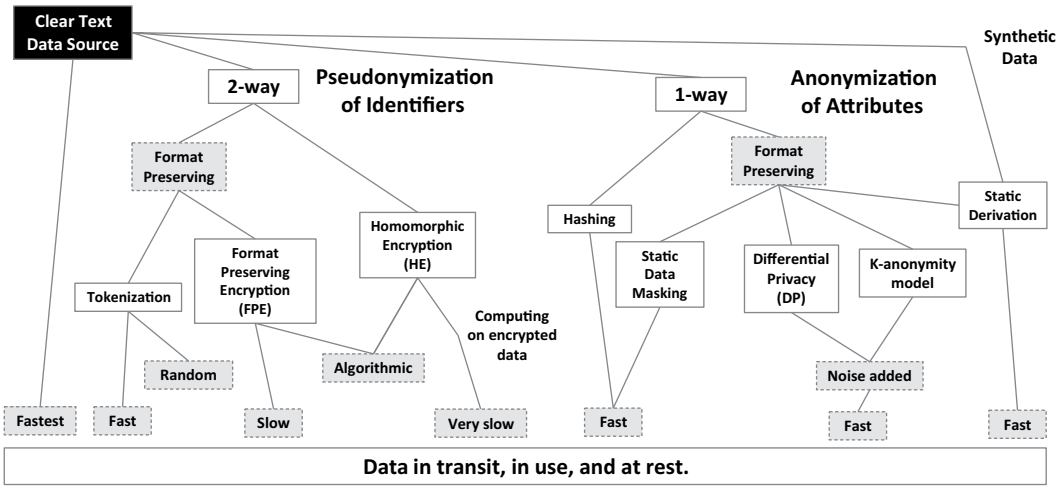


Planning for issues and benefits of quantum computing is discussed in Volume I of this book:

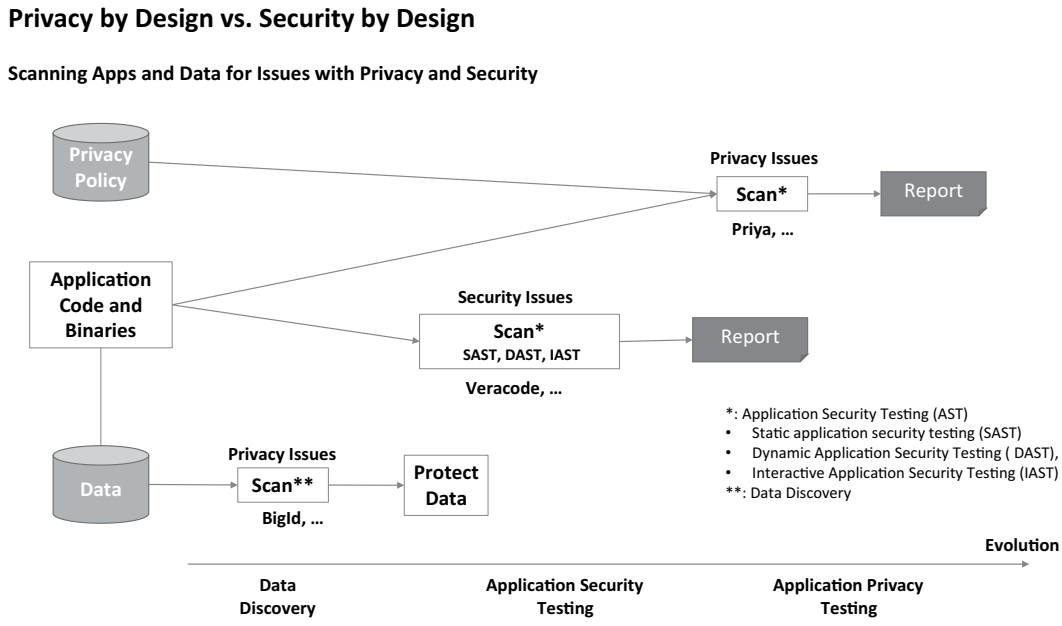


Source: Adapted from CBI Research and Gartner

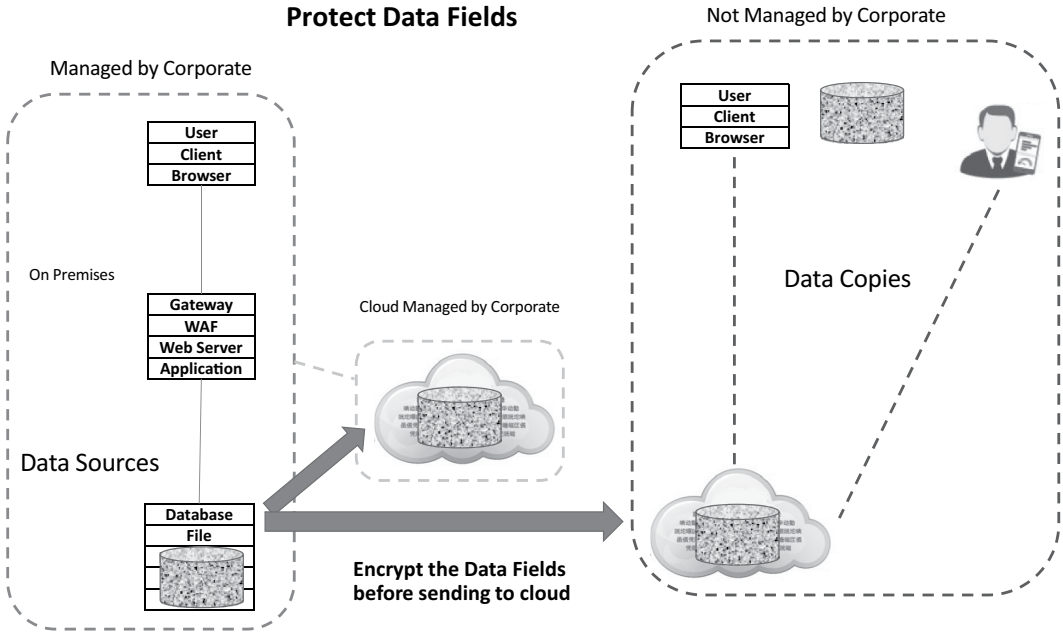
Volume I discussed different techniques for protecting data. This book will continue the journey into synthetic data. Synthetic data can be generated differently and measured in terms of risk and utility levels:



Volume I discussed basic data discovery and scan of applictions to find security issues. This book will continue the journey into collecting more context in finding privacy issues by evolving ways of scaning applications. This can also help in implementing privacy by design:

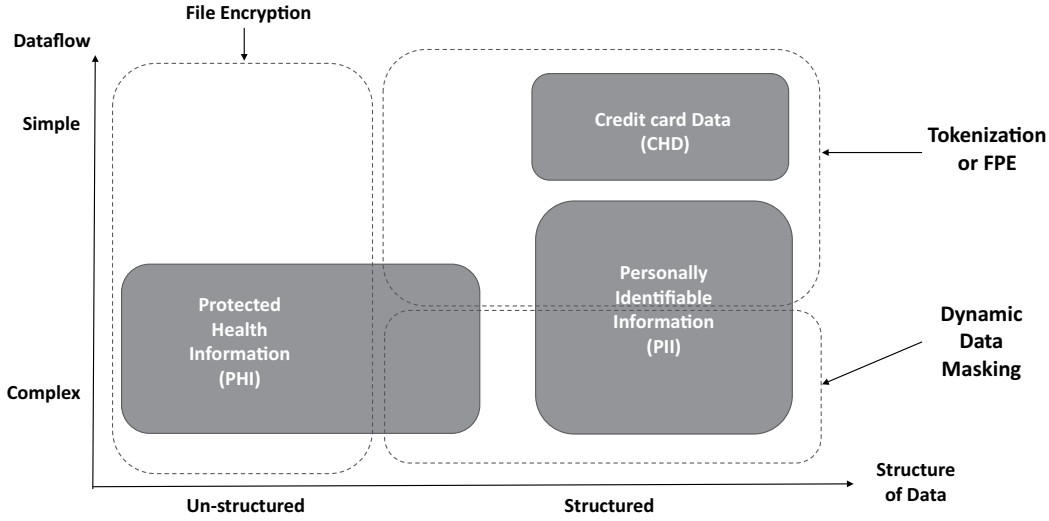


Volume I discussed basic data protection techniques for sensitive data. This book will continue the journey into applying the techniques for different use cases in cloud and increasingly distributed environments that is used by an increasingly distributed workforce:



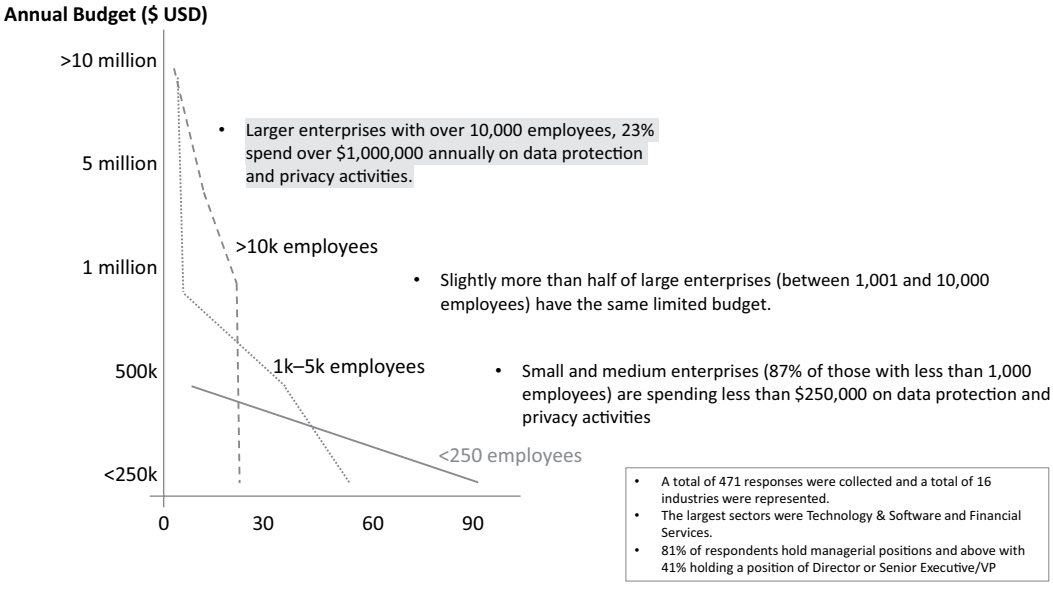
Volume I discussed basic data protection techniques for sensitive data. This book will discuss when to apply these from various data types, different types, and different use cases:

Use of different Techniques for Data Security



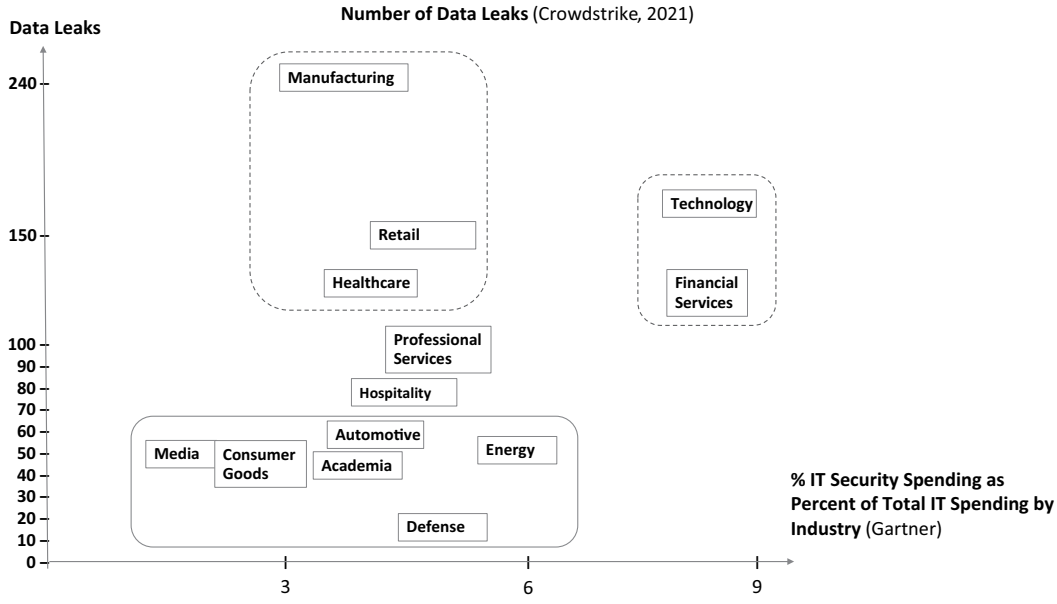
Chapter 3 discusses org structure and staffing of departments working on privacy and security for different maturity and size of organizations:

Spending on Data Protection and Privacy by Size



Source: Adapted from CPO Magazine

Chapter 3 discusses spending on privacy and security across different industries:



Chapters 2 and 3 discuss prioritization and alignment of various industry standards and guidance for different regions:

Chapters 2 and 3 position different types of product vendors that are focusing on various aspects of data privacy and security. Other vendors are focusing on consulting, emails, smaller devices, networks, or detection and response:

Example of Alignment to Standards and Guidance

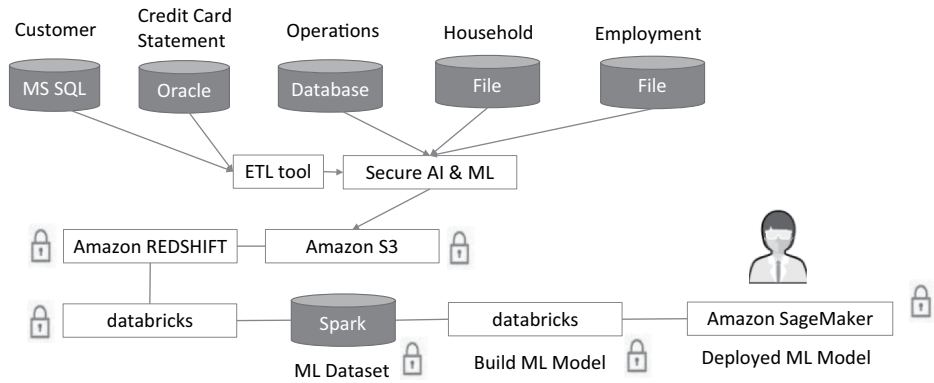
Area	Standard, Guidance, or Organization	1-Most Important			Comments	Examples of Alignment
		US	EMEA	APAC		
US National Institute for Standards and Technology	NIST SP 800-207				Zero Trust	Zero Trust Architecture
	NIST SP 800-53				Encrption and Keys	Key states, key lengths
	NIST FIPS 140-2				Encryption	Key storage, PKCS#11 integration, Level 1 encryption lib.
	NIST SP 800-171				Access Control	Access Control (PR.AC), Data Security (PR.DS)
Financial Industry Standard	PCI DSS				Payment cards Industry Standard	Encryption
	ANSI X9				Standards for the financial services industry in the U.S.	Tokenization, Encryption
Application and Encryption Guidance	PKCS				Public Key Cryptography Standard	PKCS #5, #11, #12
	Homomorphic.Computing.org				Homomorphic.Computing.org for researchers and industry (IBM, Intel, MS ...)	Future Lattice-based algorithms
	OWASP				The Open Web Application Security Project	Top 10 for API Security and WA
	CSA				Cloud Security Alliance	Quantum Computing
	CMMC 2.0				Required by US Government	Alignment with NIST SP 800-171
International Standards	ISO/IEC 27001				International Standards Organization anf International Electrotechnical Commission	ISO 27001 Annex A, or the core controls
	ISO/IEC 20889				Data De-identification	k-Anonymity
EU Data Privacy	GDPR				General Data Protection Regulation	EU Data Privacy
US Healthcare	HIPAA				Health Insurance Portability and Accountability Act	Access Control
User Groups	IEEE				The Institute of Electrical and Electronics Engineers	Integration with Data Catalogs
	CCC				The Confidential Computing Consortium	
	ISACA				Information Systems Security Association, 140k members	Journal, COBIT,
	ISSA				Information Systems Security Association	Journal
	IAPP				International Association of Privacy Professionals, comprehensive global information privacy	Journal
	(ISC)2				The International Information System Security Certification Consortium specializes in training and certifications (CISSP ...)	
	IIA				Institute for Internal Auditors	
	BCS				The Chartered Institute for IT, formerly known as the British Computer Society	
	OMG				Object Management Group	

Vendor	Email	Consulting	Devices	Network	Response	Monitor	Identity	Discover	Encrypt	Mask	Features https://www.rsaconference.com/marketplace/search#f:product=[Data%20Security]
A								Discover			discover, manage, protect, sensitive, and personal data a
B						Monitor		Discover			discover & monitor external threats
C								Discover			discover, migrate and govern
D			Devices			Monitor		Discover			discovers all endpoint devices
E						Monitor		Discover			detect and investigate threats to your most sensitive data
F			Devices					Discover			Discover, manage, and automate the lifecycle of SSH keys
G									Encrypt	Mask	CASB, SWG, and ZTNA
H									Encrypt	Mask	field-level protection
I									Encrypt		key management, tokenization, cloud key management, encryption and HSM
J									Encrypt		key management
K										Mask	Activity Monitoring, Database Firewall, Dynamic and Static Data Masking, Discovery

Chapter 3 discusses how solutions are more prescriptive to different use cases and each industry. For example, using protected data in machine learning to address fraud in the financial industry:

Use Case - Reducing Risk with Financial Data

- Anonymization minimized the risk of identification at a bank for credit card approval transactions.
- The bank reduced the **privacy risk from 26% to 8%** and still provided **98% accuracy** compared to the initial **Machine Learning** model used in the analytics.
- Anonymization is a non-reversible method of protection because it can advance data-intensive business applications, such as analytics, by using **differential privacy or k-anonymity**.
- **Pseudonymization** is a reversible approach that can be based on Encryption or tokenization.



You cannot manage what can't measure. Metrics are important. Chapter 5, for example, discusses Trust maturity:

Zero Trust Maturity Model

Areas

Identity	Device	Environment (NW)	Application	Data
Analytics				
Automation				
Governance				

Maturity Levels

Maturity	Identity	Device	Environment (NW)	Application	Data
Traditional	Password or Mult Factor (MFA)	Simple inventore	Macro segmentaion	Access based on local validation	Static control
Advanced	MFA or some Federation	Data access depends on device posture	Micro perimeters	Access based on central validation	Cloud data encrypted
Optimal	Continous realtime ML analysis	Data access depends on realtime analysis	ML threat protection	Access continously validated	All data is encrypted

Source: Adapted from CISA.org

Section I

Vision and Best Practices

1 Risks and Threats

INTRODUCTION

In this chapter, we will discuss Risks and Threats and how to Ensure that your data is private and protected in transit, in use, in memory, and at rest. We will discuss Trust and Data Breaches.

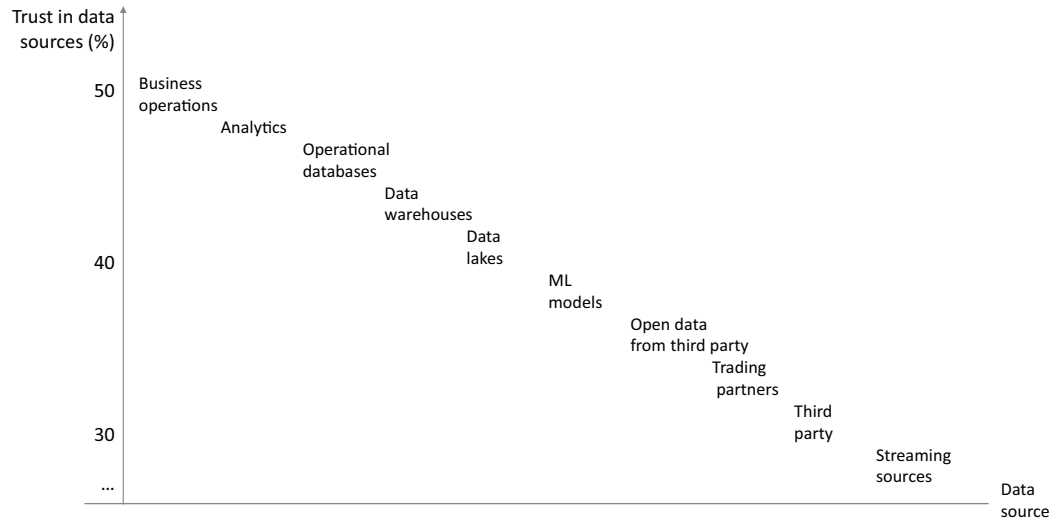
We will also discuss how to Prevent Attacks and Recover after Attacks, particularly Ransomware attacks and cloud databases.

Attackers may already be in your system. A multi-layered defense can protect your sensitive data.

A LACK OF TRUST

Trust is important for organizations to beg data-driven:

Trust is holding organizations back from being data-driven



Source: Adapted from IDC

Data powers the future enterprise in a digital-first world.

Digital-first applies to any company, government, or person that is always asking:

"Is there some digital-based capability or enhancement that could improve our lives and desired outcomes?"

A digital-first world requires business change:

98% of organizations are on a digital transformation journey.

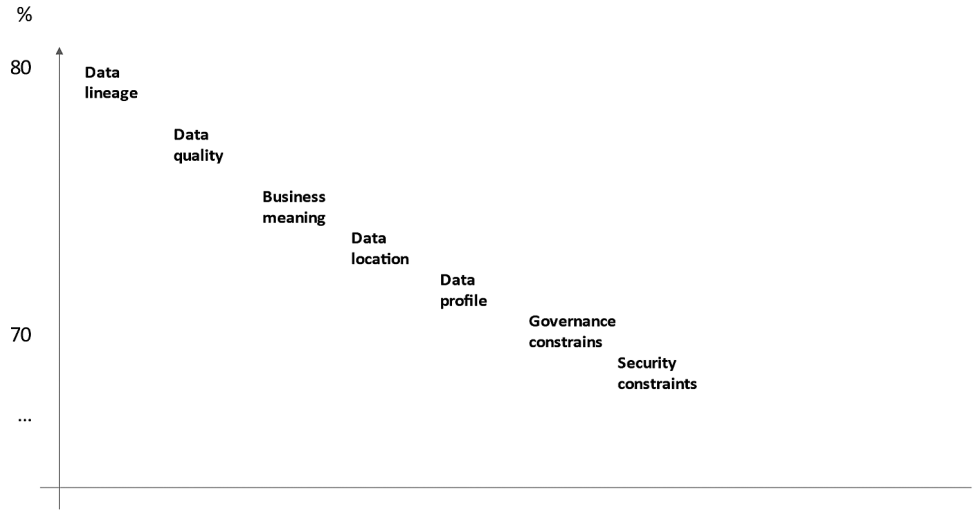
Data management is critical to digital transformation:

Organizations with solid data leadership are three times more likely to be well underway with digital transformation.

- 87% of CXOs said being an intelligent enterprise is their top priority.
- 83% of executives have articulated the need to be more data-driven than before the pandemic.

DOI: 10.1201/9781003254928-2

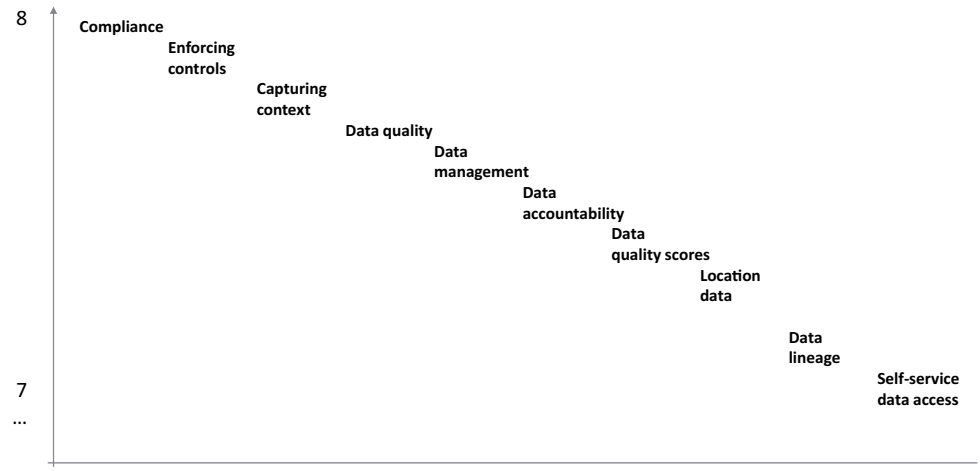
Q: When you make data-driven decisions, what do you expect and demand to know?



Source: Adapted from IDC Data Culture Survey

Q: Rate how well your organization performs

(1-10)



Source: Adapted from IDC Data Culture Survey

DATA PRIVACY

A mature privacy posture can only be achieved by using privacy management, privacy control, and (typically data-centric) security capabilities. Cutting across various disciplines, privacy is much more than a security-only discipline.

On the other hand, SECURITY leaders can proactively facilitate the achievement of Operational goals in analytics and Operational intelligence through data-centric controls like synthetic data or

differential privacy. Beyond sanctions, privacy risk mitigation focuses primarily on post-breach financial risks, consumer trust decay, and brand damage.

- According to Gartner, by year-end 2023, 75% of the world's population will have its data covered under modern privacy regulations, up from 25% today.
- Before year-end 2023, more than 80% of companies worldwide will face at least one privacy-focused data protection regulation.
- By 2024, privacy-driven spending on data protection and compliance technology will break through to more than $15 billion worldwide.
- By 2025, 60% of large organizations will use one or more privacy-enhancing computation techniques in analytics, operational intelligence, or cloud computing.

Privacy Becomes Mission Critical

Privacy has become an Operational imperative and a critical component of customer trust for organizations worldwide.

We will discuss some relevant areas of Data Security:

- Data governance, privacy, and risk, including DSG, DRA, PIA, data breach response, privacy by design (PbD), and financial data risk assessment (FinDRA).
- Data discovery, categorization, and classification of structured and unstructured data, including data classification, cloud native data loss prevention (DLP), file analysis, cloud access security broker (CASB), enterprise digital rights management (EDRM), data access governance (DAG), and multicloud database activity monitoring (Multicloud DAM).
- Data processing and analytics across endpoint, application, or storage layers, including DataOps, DevOps test data management, machine identity management, blockchain for data security, file analysis, and privacy management tools.
- Anonymization, pseudonymization, PEC, and other data protection techniques, including confidential computing, homomorphic encryption, differential privacy, format preserving encryption (FPE), secure multiparty computation (SMPC), zero-knowledge proofs, multi-cloud key management as a service (KMaaS), enterprise key management, EDRM, transport layer security (TLS) decryption platform, cloud data protection gateways, CASB, secure instant communications, and dynamic data masking (DDM).
- Monitoring access, activity, alerting, and auditing of user activity with data, including DAG, multicloud DAM, CASBs, and file analysis.
- Multicloud solutions with multifunctional data security controls, including data security as a service (DSaaS), data security platform, multicloud KmaaS, multicloud DAM.

THE THREAT LANDSCAPE

According to "Protecting Data from Ransomware and other Attacks", attacks continue to increase. The U.S. Secret Service reported that most organizations had adequate data backups. Cyber actors focus more on the exfiltration of sensitive data and threaten to publicize the data unless an additional ransom is paid.

THREAT FOR BUSINESSES

Ransomware gangs are changing. It can be very expensive for some victims, and some ransomware groups are shifting toward smaller targets.

RANSOMWARE

Prevent Attacks

ABAC (attribute-based access control) can dynamically enforce policies based on a wide range of attributes (user attributes, resource attributes, object, environment attributes, etc.) to protect data.

Data Security for Hybrid Cloud

Create data security policies and rules to protect data at rest and in transit. Use tokenization, anonymization, encryption, and other privacy models that are defined in the INTERNATIONAL DATA PRIVACY STANDARD ISO/IEC 20889. Centrally manage enterprise users and continuously monitor security behavior across hybrid cloud.

DATA BREACHES

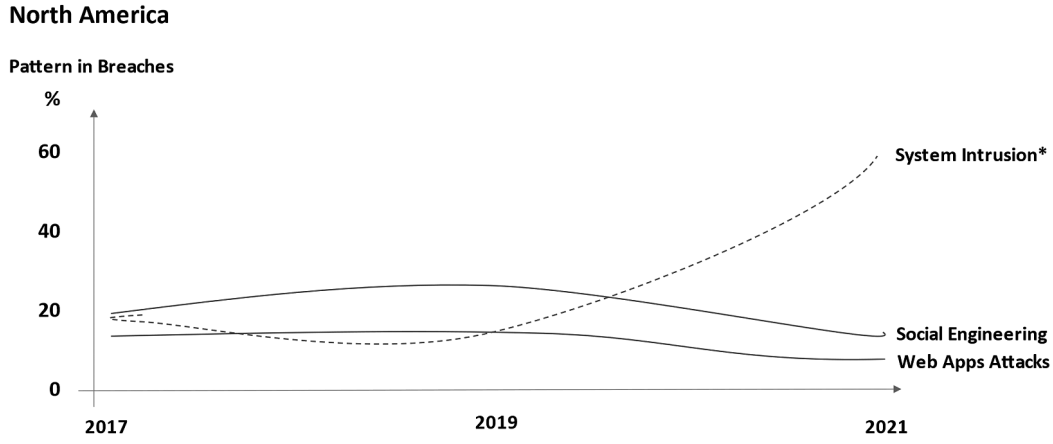
Insider Threat

According to several industry studies, insiders have caused 60% of breaches in an organization. Privileged users and third-party developers often have untethered access to some of your most sensitive data. Beyond privileged access management, restricting access to actual data values can help ensure privacy for your company's data, according to "Database and File Encryption Challenges".

Spectre-Class Vulnerabilities

Much has been written about the multitude of vulnerabilities and side channel attacks on hardware-based enclave security. While there is promise in the technology, there is also some significant risk. For organizations looking to leverage privacy-preserving analytics and confidential computing, it's important to understand what hardware-independent method can offer.

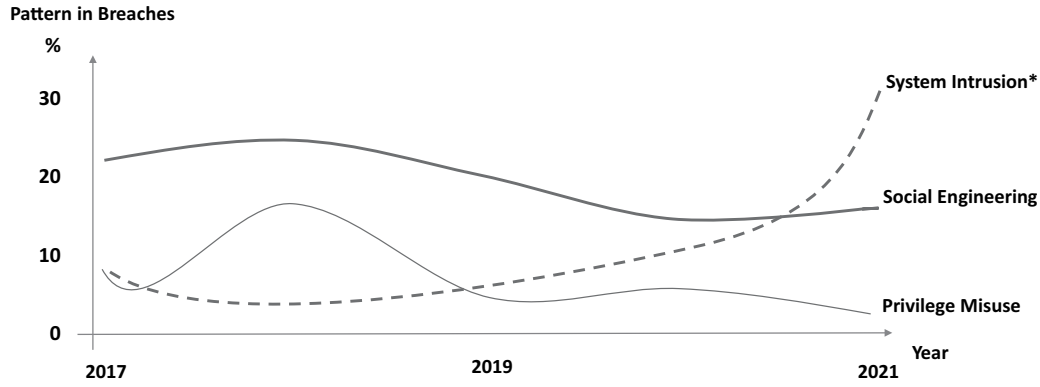
TRENDS IN DATA BREACHES



*System Intrusion is also where most of the Ransomware cases reside

Source: Adapted from Verizon DBIR, 2022

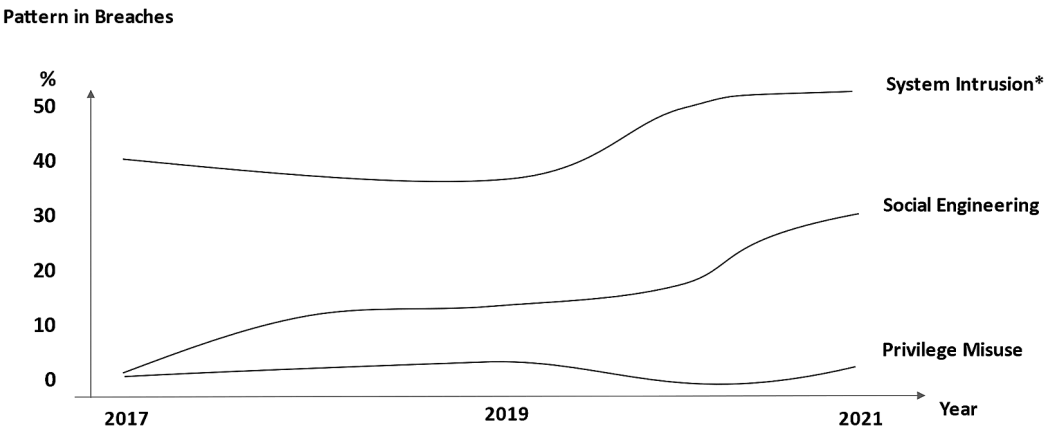
Financial Industry



*System Intrusion is also where most of the Ransomware cases reside

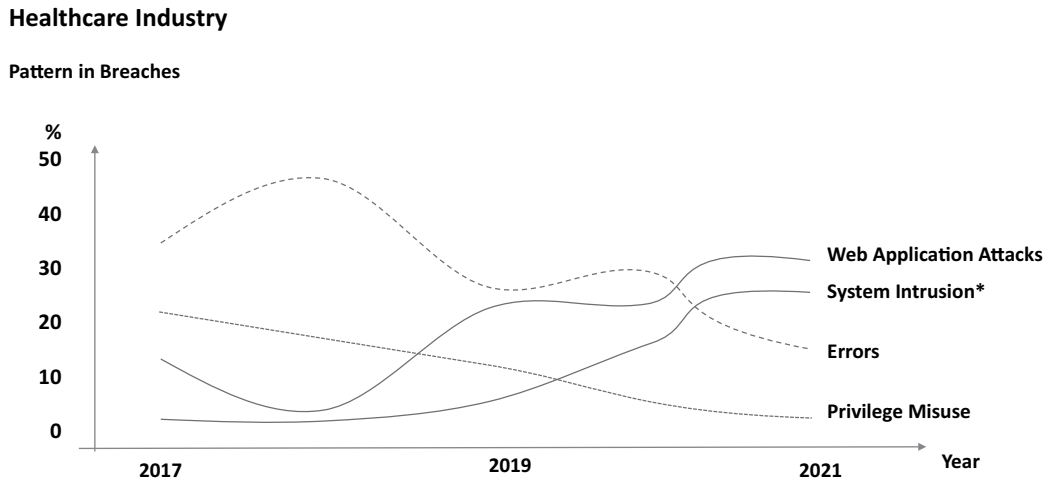
Source: Adapted from Verizon DBIR, 2022

Retail Industry



*System Intrusion is also where most of the Ransomware cases reside

Source: Adapted from Verizon DBIR, 2022



*System Intrusion is also where most of the Ransomware cases reside

Source: Adapted from Verizon DBIR, 2022

Prevent Attacks

Adopted from "NIST IR 8374 Cybersecurity Framework for Ransomware":

1. Maintain antivirus
2. Maintain patching
3. White-list apps
4. Avoid BYOD (Bring Your Own Device)
5. Run with lowest possible privileges
6. Avoid personal apps
7. Avoid unknown files
8. Avoid unknown links
9. Black-list ransomware sites

Ransomware

In 2021, targeted intrusion adversaries continued to adapt to the changing operational opportunities and strategic requirements of technology and world events.

Governments are also adapting. This year, CrowdStrike Intelligence debuted two new adversary animals—WOLF and OCELOT—to label targeted intrusions emanating from Turkey and Colombia, respectively.

Threat Landscape

The CrowdStrike Falcon OverWatch team measures breakout time—the time an adversary takes to move laterally from an initially compromised host to another host within the victim environment. Our analysis of the breakout time for hands-on eCrime intrusion activity in 2021—where such a metric could be derived—revealed an average of just 1 hour 38 minutes.

HACKTIVIST

Ransomware

According to "Ransomware in 2022: We're all screwed", Ransomware is now a primary threat for businesses, and cybersecurity experts believe this criminal enterprise will reach new heights in the

future with Colonial Pipeline. JBS. Kaseya and other victims of threat groups, including DarkSide, REvil, and BlackMatter.

According to "Ransomware in 2022: We're all screwed", the "perfect" prospective ransomware victim in the United States will have a minimum annual revenue of $100 million. Ransomware infection—including types like WannaCry, NotPetya, Ryuk, Cerber, and Cryptolocker—can be designed to elicit a blackmail payment from a victim organization.

Ransomware groups may also steal corporate data and threaten to publish or sell this information going after major profitable companies.

Ransomware-as-a-Service (RaaS)

Ransomware-as-a-Service (RaaS)—in which operators will lease out or offer subscriptions to their malware creations to others for a price—is lucrative and difficult to track down and prosecute operators.

Implications for Cyber Insurance

The cyber insurance industry is likely to go mainstream and is a simple cost of doing business. Here are a few options to consider.

The explosion in high-profile ransomware attacks is also potentially going to cause massive shifts in cyber insurance, premiums, and whether or not ransomware incidents will be covered at all.

One in Seven Ransomware Extortion Attempts Leak Key Operational Tech Records

Researchers say that double-extortion ransomware attacks represent a severe risk to operational processes.

Researchers say that one in seven ransomware extortion data leaks reveals business-critical operational technology data.

Ransomware has evolved from barebone encryption and basic demands for payment into something potentially far more severe in recent years.

MISCONFIGURING A CLOUD DATABASE

Misconfiguring a cloud database has leaked more than 14 billion data records as reported by the Breach Level Index, according to "Building Cloud Services for Security".

STEAL DATA DURING HOMOMORPHIC ENCRYPTION

According to "Researchers show they can steal data during homomorphic encryption", homomorphic encryption allows it to steal data even as it is being encrypted.

Homomorphic encryption preserves data privacy but allows users to use the data.

Microsoft, for example, created the SEAL Homomorphic Encryption Library to facilitate research and development on homomorphic encryption by the broader research community.

They found a way to "crack" homomorphic encryption by using that library via a side-channel attack.

CRYPTO CRIME TRENDS

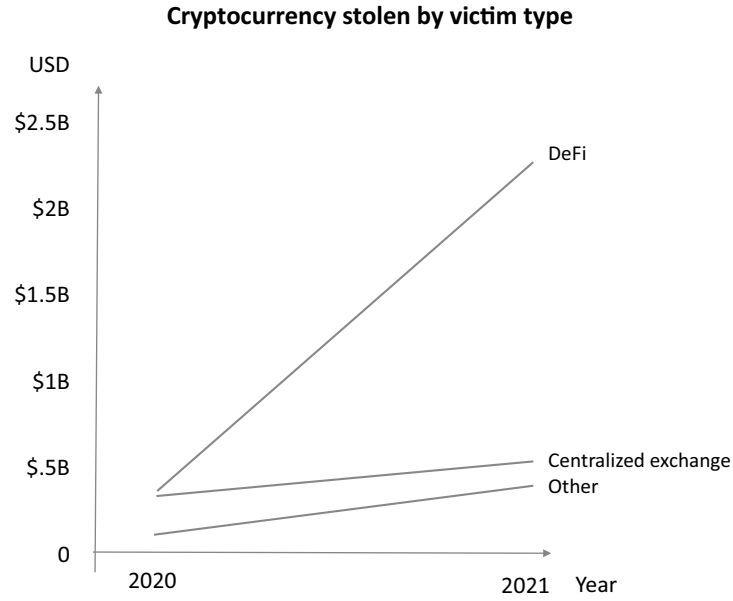
Cryptocurrency usage is growing, according to "Crypto Crime Trends for 2022: Illicit Transaction Activity".

The growth of legitimate cryptocurrency usage far outpaces the growth of criminal usage, according to "Crypto Crime: $14 Billion in Digital Currency Was Stolen".

DEFI HAS CONTINUED TO GROW

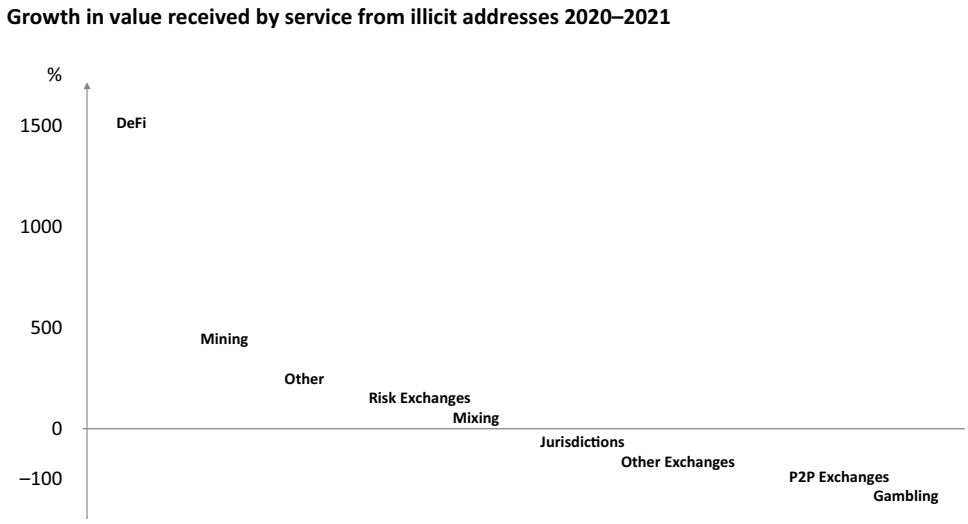
Following are the issues with stolen funds:

In 2020, just under $162 million worth of cryptocurrency was stolen from DeFi platforms, which was 31% of the year's total amount stolen.

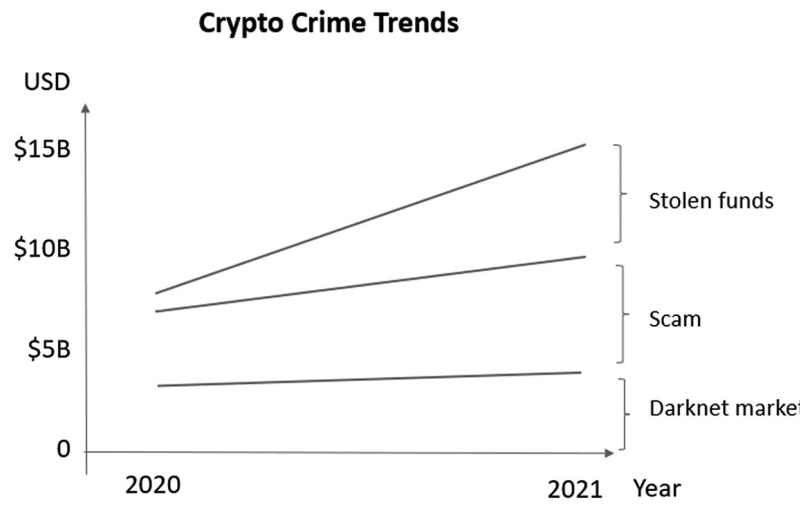


Source: Adapted from https://go.chainalysis.com

DeFi protocols showed the maximum growth by far in usage for money laundering at 1.964%. DeFi is one of the most exciting areas of the broader cryptocurrency ecosystem, presenting tremendous opportunities. But DeFi is unlikely to realize its full potential if the same decentralization that makes it so dynamic also allows for widespread scamming and theft. One way to combat this is better communication—both the private and public sectors have an essential role to play in helping investors.

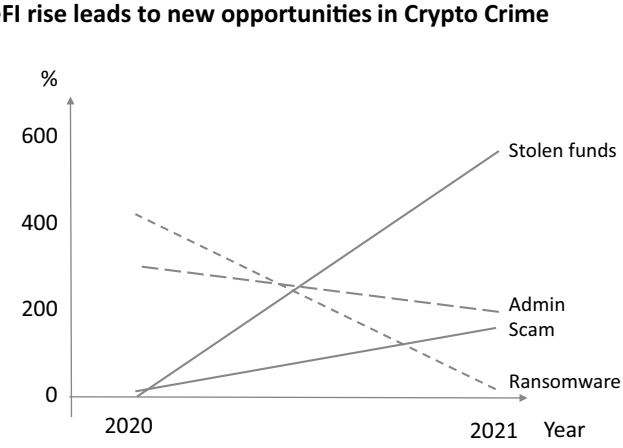


Source: Adapted from https://go.chainalysis.com



Source: Adapted from https://go.chainalysis.com

Transactions involving illicit addresses were 0.15% of cryptocurrency transaction volume. In the last Crypto Crime Report, 0.34% of 2020's cryptocurrency transaction volume was associated with illicit activity—now raised the figure to 0.62%. Law enforcement's ability to combat cryptocurrency-based corruption is also evolving. Criminal abuse heightens the likelihood of restrictions being imposed by governments and, worst of all, victimizes innocent people around the world, according to "Crypto Crime Trends for 2022: Illicit Transaction Activity".

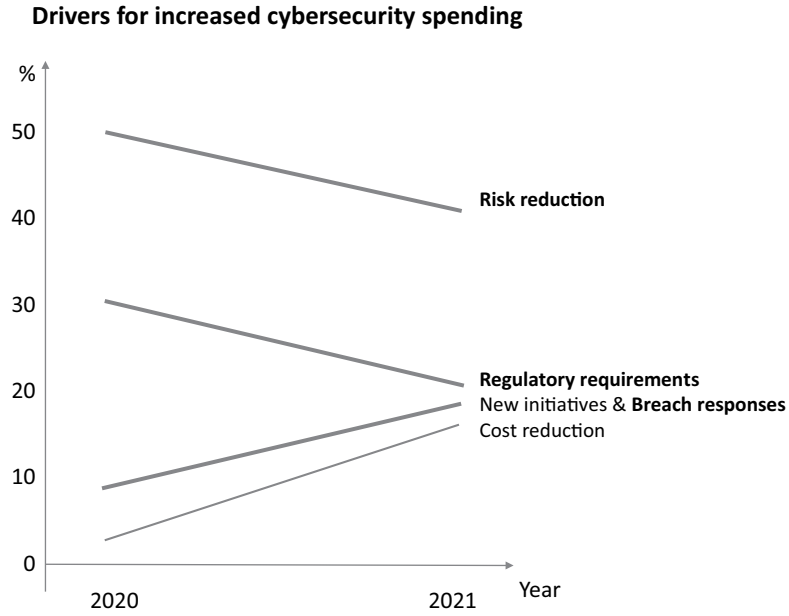


Source: Adapted from https://go.chainalysis.com

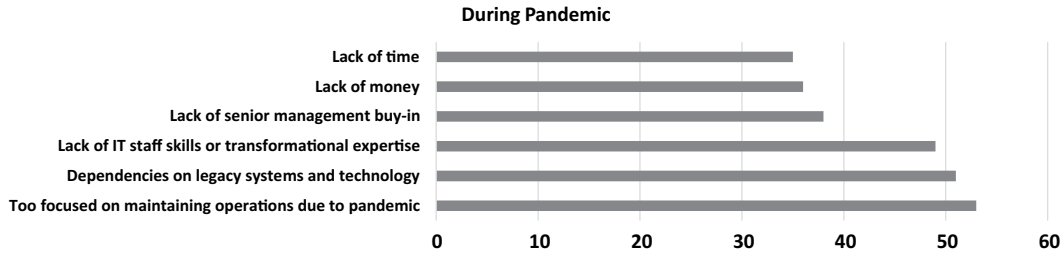
CHANGING DRIVERS FOR INCREASED CYBERSECURITY SPENDING

Risk Reduction Is Still the Top Driver

Risks and compliance are still top drivers (from 48% to 42%) and (from 29% to 18%) for increased cybersecurity spending.



Source: Adapted from EY



Source: Adapted from Gartner

FUTURE OF THE SOC

Forces Shaping Modern Security Operations

Automation is the most common way to scale. But is it effective at finding malicious acts as a manual investigation by specialists?

What has changed is more fundamental than the entrance of cloud technology. It's the role of technology in fighting the falling rate of profit. Simply put, while technology in the 20th century helped automate repeatable tasks, the role of technology in the 21st century focuses on the automation of repeatable cognitive processes, in other words—of decisions. Otherwise, automation would take care of the routine tasks, but the amount of non-routine tasks that require thinking would still overwhelm the available human analysts. It is business imperative to make the right decision faster than the competitor, according to "Future of the SOC Forces".

DATA BREACH RESPONSE

Data breach response, augmentation, and the associated disclosure are the set of activities required to assess and potentially notify regulatory authorities. Today, disclosure is mandated by omnibus

laws such as the European Union's GDPR or subject/region-specific laws, as is the case with individual U.S. state breach notification legislation.

Why This Is Important

Appropriate management of a breach-impacting personal data can substantially reduce fines (as Gartner has observed on multiple occasions) and potentially strengthen ties with affected consumers by demonstrating that the organization is proactively taking ownership of the situation. Inversely, delayed response, limited transparency, and overly legal-language-based communications often elicit regulatory investigations and are paired with reputational damage and customer loss.

NOTES

1. Cloud Security Alliance, https://cloudsecurityalliance.org/group/security-guidance/
2. Cloud Standards Customer Council 2016, Practical Guide to Hybrid Cloud Computing.
3. Cloud Standards Customer Council 2016, Public Cloud Service Agreements: What to Expect and
4. D. Proud-Madruga, "Project Summary for Privacy, Access and Security Services (PASS) Healthcare"
5. FIPS 140-2 Annex A, http://csrc.nist.gov/publications/fips/fips140-2/fips1402annexa.pdf
6. https://www.thecipherbrief.com/column/sponsored-content/crypto-crime-trends-for-2022
7. IHS 2016 Update: The Complexities of Physician Supply and Demand: Projections from 2014 to 2025
8. ISO/IEC 27017 (2015). Code of Practice for Information Security Controls Based on ISO/IEC 27002for Cloud Services. http://www.iso.org/iso/catalogue_detail?csnumber=43757
9. ISO/IEC 27018 (2014). Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors. http://www.iso.org/iso/catalogue_detail.htm?csnumber=61498
10. Japan's Updated Pharmaceutical and Medical Device Act https://www.pmda.go.jp/english/bobsguide: Cloud Target Operating Model: Revolution, Evolution or a Bit of Both?
11. https://www.sciencedirect.com/science/article/abs/pii/B9780323898249000057
12. K. Terry, "Why Telemedicine Should Be Integrated With EHRs, ACOs", Inf. Week, 2013.
13. Mckinsey & Company (August, 2016): How tech-enabled consumers are reordering the healthcarelandscape. http://healthcare.mckinsey.com/how-tech-enabled-consumers-are-reordering-healthcarelandscape
14. NIST 800-131 A, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar1.pdf
15. NIST 800-160, http://csrc.nist.gov/publications/drafts/800-160/sp800_160_second-draft.pdf
16. ONC Health I.T. Certification Program
17. Regulation (E.U.) 2016/679 of the European Parliament and of the Council (2016): E.U. General Data
18. Search Health I.T.: HITECH Act. http://searchhealthit.techtarget.com/definition/HITECH-Act
19. https://www.healthit.gov/isa/
20. U.S. Food & Drug Administration Medical Device Regulation
21. https://www.legislation.gov.uk/ukpga/1998/29/contents
22. https://www.gov.uk/guidance/on-site-access-to-electronic-health-records-by-sponsor-representatives-in-clinical-trials
23. "Building Cloud Services for Security". https://www.rapid7.com/info/3-common-misconfigurations/
24. "CrowdStrike report cites zero trust". https://insidecybersecurity.com/daily-news/crowdstrike-report-cites-zero-trust-tech-upgrades-key-combating-ransomware-threat
25. "CrowdStrike's Annual Threat Report" https://www.benzinga.com/pressreleases/22/02/b25626122/crowdstrikes-annual-threat-report-reveals-uptick-around-ransomware-and-disruptive-operations-expos
26. "Crypto Crime Trends for 2022: Illicit Transaction Activity". https://blog.chainalysis.com/reports/2022-crypto-crime-report-introduction/
27. https://finance.yahoo.com/news/crypto-crime-14-billion-digital-172810251.html?fr=sycsrp_catchall
28. "Database and File Encryption Challenges". https://baffle.io/challenges/
29. "Protecting Data from Ransomware and other Attacks". https://www.globalsecuritymag.com/Protecting-Data-from-Ransomware,20210831,115566.html
30. "Ransomware as a service: Negotiators". https://www.zdnet.com/article/ransomware-as-a-service-negotiators-between-hackers-and-victims-are-now-in-high-demand/
31. "Ransomware gangs are changing their tactics". https://asaniali.org/2022/02/07/ransomware-gangs-are-changing-their-tactics-that-could-prove-very-expensive-for-some-victims/

32. “Ransomware in 2022: We’re all screwed” ZDNet. https://www.zdnet.com/article/ransomware-in-2022-were-all-screwed/
33. “Researchers show they can steal data during homomorphic encryption”. https://techxplore.com/news/2022-03-homomorphic-encryption.html
34. “Crypto Crime Trends for 2022”
35. “Future of the SOC Forces”. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/about-deloitte/us-deloitte-google-cloud-alliance-future-of-the-SOC-whitepaper.pdf
36. 2.0. http://www.cloud-council.org/deliverables/practical-guide-to-cloud-service-agreements.htm
37. “Advisory”, CMS, Washington DC, RPRT, Aug. 2016.
38. “Audit Services Conceptual Model”. HL7, Ann Arbor, MI OR - HL7, 09-May-2016.
39. Bioinform, p. bbv118, Feb. 2016. http://dx.doi.org/10.1093/bib/bbv118
40. CDNET, Ransomware gangs are changing their tactics. https://www.zdnet.com/article/ransomware-gangs-are-changing-their-tactics-that-could-prove-very-expensive-for-some-victims/
41. Cloud Standards Customer Council 2015, Practical Guide to Cloud Service Level Agreements, Version
42. D. Major, “Million Veteran Program signs up bio analysis firm for hybrid cloud”, GCN, Apr. 2016.
43. HIPAA. http://www.hhs.gov/hipaa/
44. http://dx.doi.org/10.1016/j.jss.2013.09.012
45. http://www.cloud-council.org/deliverables/practical-guide-to-hybrid-cloud-computing.htm

SECURITY, AUDIT AND LEADERSHIP SERIES

Cognitive Risk

James Bone
and Jessie H Lee

CRC Press
Taylor & Francis Group

Cognitive Risk

Cognitive Risk is a book about the least understood but most pervasive risk to mankind – human decision-making. Cognitive risks are subconscious and unconscious influence factors on human decision-making: heuristics and biases. To understand the scope of cognitive risk, we look at case studies, corporate and organizational failure, and the science that explains why we systemically make errors in judgment and repeat the same errors.

The book takes a multidisciplinary and pedestrian stroll through behavioral science with a light touch, using stories to explain why we consistently make cognitive errors that not only increase risks but also simultaneously fail to recognize these errors in ourselves or our organizations. This science has deep roots in organizational behavior, psychology, human factors, cognitive science, and behavioral science all influenced by classic philosophers and enabled through advanced analytics and artificial intelligence. The point of the book is simple. Humans persist with bounded rationality, but as the speed of information, data, money, and life in general accelerates, we will need the right tools to not only keep pace but to survive and thrive.

In light of all these factors that complicate risk, the book offers a foundational solution. A cognitive risk framework for enterprise risk management and cyber security. There are five pillars in a cognitive risk framework with five levels of maturity, yet there is no universally prescribed maturity level. It is more a journey of different paths. Each organization will pursue its own path, but the goal is the same – minimize the errors that could have been avoided. We explain why risks are hard to discuss and why we systematically ignore the aggregation of these risks hidden in collective decision-making in an organization.

The cognitive risk framework is a framework designed to explore the two most complex risks organizations face: uncertainty and decision-making under uncertainty. The first pillar is cognitive governance, which is a structured approach for institutionalizing rational decision-making across the enterprise. Each pillar is complimentary and builds on the next in a succession of continuous learning. There is no endpoint because the pillars evolve with technology. Enterprise risk is a team effort in risk intelligence grounded in a framework for good decision-making. We close with a call to become designers of risk solutions enabled by the right technology and nurtured by collaboration.

We hope you enjoy the book with this context.

First edition published 2023
by CRC Press
6000 Broken Sound Parkway NW, Suite 300, Boca Raton, FL 33487-2742

and by CRC Press
4 Park Square, Milton Park, Abingdon, Oxon, OX14 4RN

CRC Press is an imprint of Taylor & Francis Group, LLC

Library of Congress Cataloging–in–Publication Data

Names: Bone, James (Risk advisory consultant), author.
Title: Cognitive risk / James Bone and Jessie Lee.
Description: Boca Raton, FL : CRC Press, 2023. | Series: Security, Audit and Leadership Series | Includes bibliographical references and index.
Identifiers: LCCN 2022034775 (print) | LCCN 2022034776 (ebook) | ISBN 9781032039091 (hbk) | ISBN 9781032039114 (pbk) | ISBN 9781003189657 (ebk)
Subjects: LCSH: Organizational behavior. | Risk management. | Subconsciousness.
Classification: LCC HD58.7 .B655 2023 (print) | LCC HD58.7 (ebook) | DDC 658--dc23/eng/20221122
LC record available at https://lccn.loc.gov/2022034775
LC ebook record available at https://lccn.loc.gov/2022034776

ISBN: 978-1-032-03909-1 (hbk)
ISBN: 978-1-032-03911-4 (pbk)
ISBN: 978-1-003-18965-7 (ebk)

DOI: 10.1201/9781003189657

Typeset in Sabon
by Deanta Global Publishing Services, Chennai, India

Contents

About the authors

JAMES BONE

James Bone is the president of Global Compliance Associates, LLC, an enterprise risk researcher, and the first cognitive risk consultant. Since the publication of his first book *Cognitive Hack*, James has promoted the idea of a cognitive risk framework in several publications and has developed a following on social media as a thought leader in this space. James has also served as lecturer in discipline in Enterprise Risk Management at Columbia University School of Professional Studies. *Cognitive Risk* will be the first book of its kind to apply additional research and experience through case studies to formulate a more complete cognitive risk framework for cybersecurity and enterprise risk management. James has two websites, globalcomplianceassociates.com and thegrcbluebook.com, as well as 5,000–8,000 fellow global risk professionals seeking thought leadership in risk best practices.

JESSIE H LEE

Jessie H Lee has 20+ years of leadership experience in financial, government, higher education, and nonprofit sectors. Jessie is a strategic and insightful leader who enables organizations to transform and grow through innovative and inclusive approaches integrating enterprise risk management, technology, and data to strengthen financial and operational sustainability and flexibility. She employs data-driven approaches and builds collaborative and trusted relationships with boards, executive leaders, staff, strategic partners, and industry leaders. She founded Better Future Strategies LLC to enable the nonprofit and social enterprise organizations to achieve their visions. She is the Director of Operations at Statement Arts, a nonprofit providing arts education to young people in New York City. She teaches in both Enterprise Risk Management and Nonprofit Management Masters degree programs at Columbia University.

Introduction

WHAT IS COGNITIVE RISK AND WHY IT IS RELEVANT AS WE ENTER THE DIGITAL REVOLUTION?

Cognitive risk originated in healthcare to describe cognitive decline in dementia but has become a buzzword in technology in the digital age. This book is one of the first of its kind to define the role of cognitive risks in its many manifestations in organizational behavior. Cognition is defined as "the mental action or process of acquiring knowledge and understanding through thought, experience, and the senses." Cognition encompasses many aspects of intellectual functions and processes such as attention, the formation of knowledge, memory and working memory, judgment and evaluation, reasoning and computation, problem-solving and decision making, comprehension, and production of language.[1]

Cognitive processes have been studied by researchers in a broad range of disciplines from healthcare, psychiatry, cognitive psychology, neuroscience, philosophy, education, computer science, and many others. The human mind is central to how we perceive the world, imagine new ideas, and shape our perception of danger, joy, love, and life, but it also leads us astray. This book is about the risk factors that lead to errors in judgment when we least expect it. Daniel Kahneman, an applied psychologist, popularized these risks of the human mind in *Thinking, Fast and Slow*.

Daniel Kahneman and Amos Tversky's research, *Prospect Theory*, won the Nobel Prize in Economics in 1979, a first for the applied cognitive and mathematical psychologists. Kahneman and Tversky focused on the psychology of prediction and probability judgment and formed a foundation for behavioral economics as a new discipline of study in economic research and political thought. Daniel and Amos's work popularized heuristics and bias as risks that lead to errors in judgment under uncertainty. Kahneman and Tversky were not the first to make these observations. Prospect theory emerged from rational choice theory in economics.[2] Daniel Bernoulli is credited with being the first to recognize the contradictions in the notion of *expected value* as far back as 1738.

Bernoulli was the first to introduce the concept of systemic bias in decision-making based on a "psychophysical" world. As the world transitions from a psychophysical world to a "digital" one, the rise of misinformation, conspiracy theories, social media, and the current public discourse. Cognitive risks becomes increasingly more problematic where "truth" is harder to distinguish from subjective values. Bernoulli used a simple coin toss to demonstrate the limitations of "expected value" as a normative decision rule. Bernoulli's findings are still being violated by financial analysts in insurance, market analysts, enterprise risk management, healthcare diagnoses, and prediction in political campaigns. When I use the term, "violated," in this context, what I mean is the subjective value of a payoff is not always based on the absolute amount of the payoff. Bernoulli found that the "value a person attaches to an outcome can be influenced by subjective factors such as the likelihood of winning, or probability."

Kahneman and Tversky's attention to heuristics is instructive, which are the short-cuts that we learn over time in problem-solving and self-discovery, are not optimal, but do satisfy an approximation of a correct answer, which explains why "to err is inherently human." Heuristics are the underlying cause of error, but bias is the weight we apply in favor of or against choices we make in everyday life which can magnify the error in certain circumstances. When Kahneman and Tversky are mentioned, many observers primarily focus on bias in prospect theory, when in fact, heuristics is the headliner and biases are the bit-players in decision-making. Prospect theory provides a fresh perspective on the philosophical underpinnings that trace its roots to influential thought leaders as far back as Zoroastrian-Persian and Greek scientists and philosophers.

The term "cognitive risk" is coined by the authors, not as science but as an umbrella term to describe a multidisciplinary body of research and emerging disciplines that include human factors, behavioral science, cognitive science, linguistics, choice theory, decision science, and risk management, among others. Each of these disciplines explores how humans behave, make choices, and explain the influencing factors that shape our beliefs. The goal of this book is to examine cognitive risks through case studies to begin a journey of reflection on why we have failed to learn the lessons of the past and continue to repeat the mistakes of our ancient forefathers.

Cognitive risk is introduced at a critical inflection point in history, as we transition from a work environment largely made up of manual labor, knowledge work, and eventually to a new digital operating environment. The lessons learned in the physical world must be expanded to include a whole new set of digital risks in cyberspace at the intersection of human and machine interactions. In other words, risks in a digital economy require a different way of managing and a new set of tools to assess and evaluate digital risk. Traditional risk and governance models are still rooted in 19th-century subjective assessments of risk that are ineffective and do not fully

account for cognitive risks or incorporate scientific rigor. The very reason we are "surprised" by events like the Covid-19 pandemic is because people have a hard time intuitively comprehending and evaluating the meaning of probability as defined by extremely improbable, the long tails of the bell curve.

The authors have coined the term *homo periculum* to describe a new category of risks related to cognitive blind spots. Homo periculum is similar to the concept of homo economicus, or rational man theory. Homo economicus is the portrayal of humans as agents who are consistently rational and narrowly self-interested, and who pursue their subjectively-defined ends optimally. It is a word play on *Homo sapiens*, used in neoclassical economic theories and in pedagogy.[345]

Homo periculum is presented to describe similar errors of judgment in enterprise risk and corporate governance that inhibit the mitigation of complex risks in strategic objectives. Homo periculum is the fallacy that humans possess an innate ability to consistently calculate probabilistic outcomes in managing risks in complex organizations. Luck and risk aversion play a bigger role than leadership is willing to acknowledge. Cognitive risk is a new risk practice for the digital age to examine the presence of *homo periculum* to better understand the role of human behavior as the largest contributor to organizational dysfunction and to help explain why we fail to see the onset of major risk events. Herbert Simon called this phenomenon *bounded rationality.*

Lots of books have been written on similar topics; *The Gray Rhino, The Black Swan, MoneyBall, Predictably Irrational, The Drunkard's Walk*, and hundreds more. Each time the authors have seemingly covered new ground when, in fact, each of the authors have all described the same problem that Herbert Simon, Dan Kahneman, Amos Tversky, Paul Slovic, Frank Knight, Adam Smith, and many others have explored earlier the inability to anticipate uncertainty.

This book takes a different approach. We accept that uncertainty is the wildcard that creates both opportunity and disaster. The opportunity is to harness uncertainty while minimizing the impacts. However, to do so we must understand that each of us have cognitive blind spots that may obscure risks that we do not see. If you get nothing more from this book than a better understanding of your own bounded rationality, you have begun the journey of understanding cognitive risk. Cognitive blind spots should no longer be seen as a personal weakness. Instead, this new understanding should empower readers that cognitive risks are inherent in everyone and allows leaders in all organizations to develop strategies to build resilience in organizations that technology alone cannot.

In general, we are aware of the importance of human behavior, yet we lack a yardstick for measuring its importance or the risks associated with behavior. The understanding of human behavior is subjective, at best, but

it is broadly understood that some form of heuristics and bias is inherent in all decisions we make. Now we have science as a guide.

The goal of this book is to create a new way of thinking about uncertainty and human behavior that allows for better communication and coordination of strategic goals in an uncertain operating environment. More importantly, instead of focusing solely on technology, data analytics, and the next wave of machine learning, we put the human at the center of the solution.

This book intends to delve deeper into the questions we either fail to ask or are afraid to, such as, will a singular focus on digital technologies create risks that leave us more vulnerable and fragile? As the world transitions from technology that enables productivity gains to technology that enables entertainment, collaboration, and social interaction, are we becoming temporarily sustainable and less resilient to change and disruption? As the world builds reliance on global logistics and third-party providers, global trade has become robust in economic terms but more fragile to catastrophic and minor business disruption.

The World Economic Forum describes this era in time as the *Third Industrial Revolution*, a $200 trillion digital revolution. The world is moving forward with one foot still firmly planted in a 19th century analog world, and the other foot racing toward a new digital world, but are we simply straddling risks that are being ignored or we fail to see? ***YES!*** The symptoms are telling and wrought with the seeds of future impacts that take a toll on the human psyche and disrupt business models. There are more questions than answers which seem fitting. The rise of artificial intelligence, cyber risk, Internet of Things, and social and political upheaval creates anxiety and unease about the future.

As the world approaches the third anniversary of the COVID-19 pandemic, social media has been implicated as one example of these emerging digital risks but not the only one. This book is important if you are attempting to navigate the massive upheaval of the Digital Revolution. More importantly, this book is about understanding how to empower yourself and associates as global citizens interested in improving how your family, organization, or peer group evolves during this Third Industrial Revolution.

The idea for this book germinated in 2016, during the writing of another book, *Cognitive Hack: The New Battleground in Cybersecurity and Enterprise Risk Management*. In my search for metrics to quantify risk in cybersecurity, I discovered the biggest vulnerability is actually human error and judgment. Stunned at this finding, I was driven to learn more about the role of human error and judgment.

When considering the challenges mankind has faced over many millennia, the focus has primarily been on mankind's quest to conquer the physical elements of land, sea, space, and weather. The quest to contain the elements is still not complete, yet humans have learned to adjust and

improvise. The greatest challenges we now face are increasingly caused by humans. Humans are directly and indirectly responsible for creating some of the largest systemic risks faced by mankind: global pandemics, cyber risks and privacy, hunger, poverty, climate change, pollution, corporate failure, racism and bigotry, war, and the list is getting longer each decade.

This book is written in the hopes that a more thoughtful conversation will begin with humility, *that what we think we know may not be all there is*. The lessons of the past were hard fought through trial and error but are easily forgotten by the next generation. This is the frailty of the human mind. Sir Isaac Newton is credited with many sayings but there are two that are most relevant here. The first is, "I can calculate the motion of the heavenly bodies but not the madness of people." This quote is still as prescient today as it was in Newton's time and is the basis for this book.

The second quote is the opportunity that lies before us: "Truth is ever to be found in the simplicity [of things], and not in the multiplicity and confusion of things."

NOTES

1. https://en.wikipedia.org/wiki/Cognition.
2. https://www.press.umich.edu/pdf/0472108670-02.pdf.
3. https://www.city-journal.org/html/not-quite-rational-man-15130.html.
4. https://en.wikipedia.org/wiki/Rational_choice_theory.
5. https://www.jstor.org/stable/223329?seq=1.

Chapter 1

Reimagining the organization

Homo periculum (Human risk)

This book is about how to enhance organizational performance by avoiding massive risk failure, especially when risks are hiding in plain sight. To illustrate this point, each chapter will be divided into three parts. Part 1 will describe the problem using failure in a case study format; part 2 will create a cognitive map of the inflection points that led to failure; and part 3 will decode the cognitive risk failure and propose loosely structured approaches with intentional control design to influence behavior. The three parts are designed to encourage thinking about how to apply the lessons from the case studies to improve organizational performance, risk governance, and complex risks like cybersecurity.

Reimagining the organization requires a human-centered approach and tools to keep pace with complexity. A human-centered approach is a process of discovery in performance-hindering risks. Risk professionals aren't asking the right questions. What are the risks that hinder performance? How well do we really know our risks? Am I investing in the right risk technology? Is the work process efficient? What does risk governance look like? How do we build scale in people.

Performance-based risk analysis is an enterprise-wide approach. The ESG movement is changing how organizations perceived their impact on the environment. ESG is paving a way forward, not ERM, but something is missing in both. Metrics are being gathered to demonstrate sustainable processes across the organizational footprint but what metrics are being gathered for the impacts on people? Few of the ESG goals will be met without proactivity influencing the right behaviors in employees, customers, suppliers, and more. The common denominator in all organizations is people, and governance plays the biggest role in driving the right behaviors and influencing good decision-making to achieve corporate and environmental goals for sustainable operations. But are we asking the right questions?

Where are the biggest pain points to people – employees and customers? How can we reduce or remove friction and costs in the back office? What are the strategies to enhance uncertainty management through better people management? Do we invest in the right skills and expertise to retain top talent who know how to build high-performing teams? How best to create

DOI: 10.1201/9781003189657-1

an environment of competitiveness in excellence and support for growth? The two biggest organizational risks are performance and expectations. The tools for managing performance and expectations require a human-centered approach.

Tone at the top is often mentioned as the key to successful outcomes, but really, a positive tone is needed at all levels of the organization in order to drive positive organizational culture. Business leaders often quote sports analogies focused on individual talent, such as "Best athlete" and "Team player." Yet many fail to create an environment that allows all people to succeed. Teams, win or lose in team sports, not individuals, and teams with talent disappoint when the "chemistry" created by management is poorly managed. Teams have both superstars and position players all who contribute to success. When organizations underappreciate the role position players contribute to success, the wrong kind of tone is set. Setting the right tone across an organization enhances performance in profound ways.

Setting the right tone is about creating an environment of excellence in execution and the right tools to solve problems. One of the key tools is organizational behavior. However organizational behavior is in flux today. The Great Resignation is signaling trouble in organizational behavior that has been ignored for decades.[1] Part of the problem is organizational hierarchy and 19th-century risk governance practices that have made organizations risk averse, less innovative, and bureaucratic.[2] To examine how organizations became rigid and inflexible, we must first consider corporate governance.

CONFUSION IN ENTERPRISE RISK PRACTICE

In 1985, the Committee of Sponsoring Organizations was formed to sponsor the National Fraudulent Financial Information Commission (the Treadway Commission). The Treadway Commission was sponsored and jointly funded by five major professional accounting associations and institutes based in the US: American Institute of Certified Public Accountants (AICPA), American Accounting Association (AAA), Financial Executives International (FEI), Institute of Internal Auditors (IIA), and Institute of Management Accountants (IMA).

The Treadway Commission recommended that the sponsoring organizations of the Commission work together to develop an integrated guidance on internal control. These five organizations formed what is now called the Committee of Sponsoring Organizations (COSO) of the Treadway Commission.[3,4,5]

In the mid-1970s, the US experienced widespread questionable corporate campaign finance and corrupt foreign practices which caused the Securities and Exchange Commission to enact the Foreign Corrupt Practices Act (FCPA) of 1977.[6] FCPA was enacted for the purpose of making it unlawful for certain classes of persons and entities to make payments to foreign government officials to assist in obtaining or retaining business. The anti-bribery

provisions of the FCPA have applied to all US persons and certain foreign issuers of securities. With the enactment of certain amendments in 1998, the anti-bribery provisions of the FCPA now also apply to foreign firms and persons who cause, directly or through agents, an act in furtherance of such to take place within the territory of the US.

The FCPA also requires companies whose securities are listed in the US to meet its accounting provisions. These accounting provisions, which were designed to operate in tandem with the anti-bribery provisions of the FCPA, require corporations covered by the provisions to (a) make and keep books and records that accurately and fairly reflect the transactions of the corporation and (b) devise and maintain an adequate system of internal accounting controls. Congress never requested a risk standard to be added.

Congressional hearings on the causes of the failures focused on what could have been avoided by, among other things, *better audit practice*. Concerns about independent public accounting and audit practice are a recurring theme in corporate financial malfeasance, a topic to be returned to later. David S. Ruder, the Chairman of the Securities and Exchange Commission, emphasized "the role of internal audit in deterring, detecting, and reporting financial frauds"; however, the Commission Report went further.

The Treadway Commission set forth three major objectives: (excerpts are summarized here)

(1) To understand the extent to which fraudulent financial reporting damages the integrity of financial reporting, determine how fraud can be prevented, deterred, or detected sooner, and assess whether fraud is a product of a decline in professionalism of corporate financial officers and internal auditors; and whether the regulatory and law enforcement environment unwittingly tolerated or contributed to these types of fraud.
(2) Examine whether the role of the independent public accountant in detecting fraud had been negligent or lacked sufficient focus and determine whether changes to independent public accounting and internal audit practices can be enhanced through changes in audit standards and procedures to reduce the extent of fraudulent financial reporting.
(3) Identify attributes of corporate structure that contribute to fraudulent financial reporting or to the failure to detect such acts promptly.

The Treadway Commission recommendations targeted three groups: (a) public companies; (b) independent public accountants, and (c) the SEC.

(1) Public companies were recognized as accountable for preparing accurate financial statements, setting tone at the top, oversight of internal accounting and audit, establishment of a board audit committee, preparing management and audit committee reports, seeking out second

opinions from independent public accountants, and preparing quarterly reporting.

(2) Independent public accounting was recognized for playing a "crucial" role in detecting and deterring fraud, improving the effectiveness of the independent public accountant, and recommended changes in auditing standards, changes in procedures that enhance audit quality, improving communications about the role of independent public accountant, and changes in the process of setting audit standards.

(3) The Treadway Commission suggested to the SEC that improvements could be made in the area of fraudulent financial reporting including:
   a) increased deterrence using new SEC sanctions,
   b) greater criminal prosecution,
   c) improvements in regulation of the public accounting profession, and
   d) improvements by state boards of accountancy

The Treadway Commission also referenced two final recommendations related to the perceived liability and insurance crisis to be addressed. Additional recommendations suggested that individuals involved in the financial reporting process could benefit from "education to enhance the knowledge, skills, and ethical values that potentially may prevent, detect and defer fraudulent financial reporting." Accordingly, the report recommended changes in business and accounting curricula, professional certification examinations, and continuing professional education to achieve the goals of the Commission.

The final report is only 37 pages long which included 49 specific recommendations by the Treadway Commission.[7] The Treadway Commission study was published in 1987, and in the fall of 1992, a four-volume report entitled "Internal Control: Integrated Framework" was completed. The Treadway report presented a common definition of internal control and provided a framework against which internal control systems can be evaluated and improved. This report is guidance that US companies use to assess their compliance with the FCPA. This last statement is instructive and confirms the narrow scope of the COSO internal control integrated framework (ICIF). However, according to a survey conducted by online magazine *CFO* published in 2006, *82% of respondents said they used the COSO framework for internal controls, supposedly to comply with FCPA*.

It is reasonable to assume that expanding internal controls more broadly beyond FCPA would occur to include other areas of financial reporting as well. COSO's audit and internal controls guidance has remained fundamentally unchanged for 36 years, a focus on financial reporting and gathering evidence to attest to management's statements in financial reports. However, a 2020 study found that only 20% of respondents used COSO's guidance, and of those firms, only partial implementation is conducted.[8]

COSO published an addendum to the Reporting to External Parties volume of the COSO report. The addendum discusses the issue of, and provides a vehicle for, expanding the scope of a public management report on internal control to address additional controls pertaining to safeguarding of assets. In 1996, COSO issued a supplement to its original framework to address the application of internal control over financial derivative activities.

The COSO framework defined internal control as "a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives" in three categories – effectiveness and efficiency of operations; reliability of financial reporting; and compliance with applicable laws and regulations. COSO's integrated internal controls framework includes the following components –

> the control environment, risk assessment, control activities, information and communication, and monitoring. The scope of internal control therefore extends to policies, plans, procedures, processes, systems, activities, functions, projects, initiatives, and endeavors of all types at all levels of a company.

The COSO ICIF is definitional in nature, neither procedural nor prescriptive, which leads to confusion and disparate results in implementation. There was vigorous debate and confusion surrounding the definition of internal control over financial reporting. The guidance COSO issued on ICIF was clarification to assist with the scope of compliance. Notwithstanding the confusion, management has sole responsibility for adhering to this interpretation and public accountants are responsible for audit attestations in evidence to management's statements in financial statements.

A source of confusion has been the use of the term "risk assessment" in the COSO definition of internal controls over financial reporting. COSO's guidance includes risk language but fails to clarify the meaning of the term. For example, risk assessment as defined by COSO, "risks are analyzed, considering likelihood and impact, as a basis for determining how they should be managed. Risk are assessed on an inherent and residual basis." The definition leaves room for wide and varied interpretation which is a weakness of the COSO framework.

How should internal control risks be analyzed? Who should analyze the risks? What methods are most effective at analyzing the risk of internal control failure? What is an acceptable level of risk in internal controls? COSO fails to address these relevant questions nor define what is an "ineffective" or "effective" control. As a result, no training or expertise is needed to follow the guidance leading to disparate and varied results. Some risk professionals like the vagueness of COSO's guidance; however, a troubling

increase in fraudulent financial reporting and corporate failure is the ultimate legacy of its framework.

A statutory requirement did not come into effect until 2002, after another series of financial accounting scandals in the late 1990s and early 2000s, in the Sarbanes–Oxley (SOX) Act of 2002. SOX holds both registered public accounting firms and management of public companies ultimately accountable for the accuracy of financial statement reporting.[9] Section 404 of the Sarbanes–Oxley Act established a new rule that required management to include in their annual reports a certification of management's assessment of the effectiveness of the company's internal control over financial reporting.[10]

The annual report of management on the company's internal control over financial reporting has several key requirements (only summaries provided): (a) a statement of management's responsibility to establish and maintain adequate internal controls; (b) a statement of management's assessment of the effectiveness of internal controls; (c) a statement identifying the framework used by management to assess the effectiveness of internal controls; and (d) a statement that the registered public accounting firm that audited the firm's financial statements include in management's annual report an attestation report on management's assessment of the company's internal controls over financial reporting. The COSO framework is not a standard, it guidance for management, and many executives are not aware of the type of framework used to assess the effectiveness of internal controls.

The Treadway Commission recognized the root cause of fraud as the behavior of independent public accountants, internal audit, and corporate executives in fraudulent financial reporting. The final Treadway report documented the debates and finger-point that ensued afterward ensuring that many of the recommendations were delayed or watered down until 2002 when Congress enacted the Sarbanes–Oxley Act. Many of the Treadway Commission's recommendations were codified into new legislation in SOX 2002. Ten years after the Treadway Commission, fraud grew exponentially worse, not better! Counterintuitively, COSO has benefited from the increasing frequency of fraud by pivoting to consulting on failure in internal controls over financial reporting.

COSO's member firms began promoting integrated internal controls as a *risk* framework with other Big Four Accounting firms, selectively chosen academics, and external consultants to promote risk-based audits. The risk communication has always been troublesome and fraught with a variety of conflicting definitions and meanings. Depending upon one's point of view, one person's perception of risks can mean different things to different people. COSO's generic risk language means that anything can be a risk without rigorous probabilistic confidence levels or rules-based guidance. Subjectively defined assessments of risk has led unintended rigidity under the guise of risk management leading to a culture of risk aversion as opposed to a culture of compliance.

Auditors are responsible for managing *audit risks*, not business risks. The biggest risk to registered independent public auditors is a failed audit; fraud, misstatements of financial reports, and failure to identify accounting malfeasance. The AICPA defines an auditor's role in assessing audit risk.[11]

This Audit Risk Assessment Tool (ARAT) is designed to provide illustrative information with respect to the subject matter covered and is recommended for use on audit engagements that are generally smaller in size and have less complex auditing and accounting issues. It is designed to help identify risks, including significant risks, and document the planned response to those risks. The Audit Risk Assessment Tool should be used as a supplement to a firm's existing planning module whether in a firm-based or commercially provided methodology. The Audit Risk Assessment Tool is not a complete planning module.

The AICPA recommends the Audit Risk Assessment Tool be completed by audit professionals with substantial accounting, auditing and specific industry experience and knowledge. For a firm to be successful in improving audit quality and efficiencies, it is recommended that an auditor with at least five years of experience complete the Audit Risk Assessment Tool, or the engagement team member with the most knowledge of the industry and client (often Partner in small or medium firms) provide insight to whomever is completing the Audit Risk Assessment Tool. The AICPA recommends this should not be delegated to lower-level staff and just reviewed—it should be completed under the direction of the experienced auditor (if you delegate to inexperienced auditor, you will be at risk for less effectiveness and efficiencies because the tool is intended to be completed by an experienced auditor).

The Audit Risk Assessment Tool does not establish standards or preferred practices and is not a substitute for the original authoritative auditing guidance. In applying the auditing guidance included in this Audit Risk Assessment Tool, the auditor should, using professional judgment, assess the relevance and appropriateness of such guidance to the circumstances of the audit. This document has not been approved, disapproved, or otherwise acted on by a senior committee of the AICPA. It is provided with the understanding that the staff and publisher are not engaged in rendering legal, accounting, or other professional service. All such information is provided without warranty of any kind.

The AICPA is clear that audit risks are the primary role of auditors and only "experienced" auditors should use the Audit Risk Assessment Tool. The ARAT is not a rigorous risk assessment tool to be used beyond the scope of an audit and guided by experienced senior auditors. It is however easy to see why there has been confusion about the role of audit in risk assessment and risk management as the scope of work auditors are asked to do has expanded. The problem is that the tools auditors have at their disposal are inadequate for an effective risk assessment and are recognized in the AICPA guidance above. Misinterpretations of this guidance and the misuse

of risk language have resulted in unnecessary costs and poorly inadequate risk programs.

SOX added further confusion in its requirement on the formation of an audit committee on corporate boards. The Sarbanes–Oxley Act of 2002 mandates that audit committees be directly responsible for the oversight of the engagement of the company's independent auditor. Securities and Exchange Commission (the Commission) rules were designed to ensure that auditors are independent of their audit clients.[12] Guidance from the Securities and Exchange Commission is clear cut:

> The Commission's general standard of auditor independence is that an auditor's independence is impaired if the auditor is not, or a reasonable investor with knowledge of all the facts and circumstances would conclude that the auditor is not, capable of exercising objective and impartial judgment on all issues encompassed within the audit engagement. To determine whether an auditor is independent under this standard an audit committee needs to consider all of the relationships between the auditor and the company, the company's management, and directors, not just those relationships related to reports filed with the Commission. The audit committee should consider whether a relationship with or service provided by an auditor:
> (a) creates a mutual or conflicting interest with their audit client.
> (b) places them in the position of auditing their own work.
> (c) results in their acting as management or an employee of the audit client; or
> (d) places them in a position of being an advocate for the audit client.

Confusion in the interpretation of the guidance above has extended to the role of the audit committee. The SEC guidance for the audit committee did not intend it to become a de facto "risk committee." The role outlined by the SEC, as described above, is to ensure independence in the auditor's duty.[13] However, the audit committee's role is impaired by an increase in advisory and consulting relationships between the auditor and the company. The lines have been blurred to the extent that conflicts in the relationship between external auditors and the firm have become difficult to untangle.

The risk of "mutual and conflicting interests" is widespread when independent auditors are consulting on risk management, the sole responsibility of management, or providing other services that lend themselves to place the audit firm in a position of being an advocate for the audit client. The rules are intended to limit and prevent conflicts, yet these same conflicts continue to be the cause of financial fraud and business failure. The extent of the damage in misaligned interpretations of the rules created by auditor role expansion has become substantial in material loss in shareholder value and jobs when companies fail and litigation ensues.[14]

The original mandate given to the Treadway Commission was completed in 1992 when its report was issued. The report was designed to ensure *compliance* with the Foreign Corrupt Practices Act, a very narrow remit. Typically, when a Blue Chip panel has completed its task, the group is dissolved; however, the COSO group has persisted for 36 years. A detailed review of deliberate actions taken by the COSO board will demonstrate how the nonprofit remains a platform for generating consulting fees for independent public accounting firms.

The role of corporate risk functions was nonexistent or newly forming in the early-1990s and 2000s. Large financial services firms implemented market, financial, and credit risk departments, but operational risk management did not take shape until much later in the Basel Capital Accord formulated by Central Bankers. Many of these risk functions operate as silos without active engagement between the different disciplines, but recent changes have shown that enterprise risk functions are slowly evolving. Enterprise-wide risk management (ERM) is a process of coordinated risk management that places greater emphasis on co-operation among departments to manage an organization's range of risks as a whole. Enterprise-wide risk management is still an aspirational goal for most organizations with some progress noted. While COSO's ERM integrated framework (IF) has captured public attention as the most popular, the reality is that few organizations adhere to COSO's guidance and instead use a hybrid of risk practices to achieve an enterprise view of risks.

Several industries still do not have formal risk programs. Public accounting firms benefit from covering a broad swath of industries and internal operations. This perspective gives its members a ringside view of risk practice across diverse firms along with insights on management's expectations about the lack of leadership in risk practice broadly. COSO filled a gap in uncoordinated efforts in risk practice given its position on the audit committee of corporate boards.

Congressional legislation in Sarbanes–Oxley was designed to clarify the narrow scope of audit and public accounting firms after Enron, WorldCom, and Tyco revealed the complicity of audit behavior in fraudulent financial reporting.[15] Title I of Sarbanes–Oxley established the Public Company Accounting Oversight Board to monitor and inspect registered public accounting firms, evaluate audit quality, and administer discipline if necessary. Title II of SOX mandated auditor independence to avoid conflicts of interest, among many other requirements.

Fraud, executed through the manipulations of systems, people, and processes, is a significant risk to organizational survival, but it is one risk among many shared in all organizations. A financial risk exists if the principals of a firm choose to commit fraud. The risk of not detecting, deterring, preventing, and correcting this one risk, which can take many forms, is a significant business risk. However, fraud is a business risk the Treadway Commission

and the SEC delegated to management, internal audit, independent public accountants, and the SEC to address. COSO's framework works only when people are committed to ethical behavior and follow acceptable accounting practice. One of the key concepts in the COSO integrated internal control framework is, internal control is carried out by people. It is not simply about policies, manuals, and forms, but about people at all levels of an organization.

However, in the same guidance, the limitations of COSO's framework are described here: Internal control involves human action, which introduces the possibility of errors in prosecution or trial. Internal control can also be overridden by collusion among employees (separation of duties) or coercion by senior management.

The magazine *CFO* reported that companies are struggling to apply the complex model provided by COSO. "One of the biggest problems: limiting internal audits to one of the three key objectives of the framework. In the COSO model, these objectives apply to five key components (control environment, risk assessment, control activities, information and communication, and monitoring "Given the number of possible matrices, it is not surprising that the number of audits can get out of control." CFO magazine continued to state that many organizations are creating their own risk and control matrix by taking the COSO model and modifying it to focus on the components that relate directly to Section 404 of the Sarbanes–Oxley Act."

In fact, a 20-year COSO study of fraud, since the enactment of COSO's ICIF, found that the occurrence and magnitude of fraud exploded over the 20 years since the enactment of COSO's ICIF.[16] In fact, the detection of fraud is more likely than not from an internal whistleblower than from internal audit or independent public accounting firms. Fraud risk is one of many financial risks inherent in all for-profit and nonprofit organizations alike. Human behavior is the risk not internal controls.

The fact that COSO's framework is not a risk management framework does not minimize the importance of this work. Naming ICIF a risk framework has created significant confusion in the emphasis placed on compliance versus the analysis of risk in the business broadly. The confusion created in audit's role should be settled to allow for advancements in both regulatory compliance and business risk analysis, separately and in collaboration. The attention and resources spent on compliance risks have created organizational rigidity, bureaucracy, and risk aversion.

It is important to understand how COSO and public accounting firms grew into a dual role: on the one hand, providing assurance services to external stakeholder on the accuracy of financial reporting; and on the other hand, acting as advisers and consultants on enterprise risk and other advisory services. These dual roles create inherent conflicts the SEC warns boards to be cognizant of and proactively address. Confusion, complexity, and complacency have led to the adoption of a framework designed to address a very narrow compliance mandate (bribery) became adopted as a

"*one-size-fits all*" risk solution without any substantive evidence of efficacy in risk mitigation.

COSO's guidance points out these weaknesses:

> although business risk management provides significant benefits, there are limitations. Business risk management depends on human judgment and, therefore, is susceptible to decision making. Human failures, such as simple errors or errors, can lead to inadequate risk responses. In addition, controls can be voided by collusion of two or more people, and management can override business risk management decisions. These limitations prevent a board and management from having absolute security regarding the achievement of the entity's objectives.[17]

Philosophically, COSO is more oriented toward controls [compliance]. Therefore, it has a *bias* toward risks that could have a negative impact instead of the risk of missed opportunities.[18] The bias of negative outcomes creates risk-averse behavior while ignoring upside opportunities in informed risk-seeking behavior. To better understand the performance of COSO's guidance on the mitigation of fraudulent financial reporting, I reviewed the results from internal studies COSO published in 2010.[19,20]

In 2010, COSO published a nine-year study called "Fraudulent Financial Reporting – 1998-2007: An Analysis of US Public Companies."[21,22] A summary of the 2010 report was published by the North Carolina State Poole College of Management. The 2010 study was the last of only two studies conducted by COSO. The first study covered the years 1987–1997 and included a small sample of 294 cases of fraud. The 2010 study sample size included 347 cases of alleged fraudulent financial reporting.

Excerpts of the summary are presented here:

- The dollar magnitude of fraudulent financial reporting soared in the last decade, with total cumulative misstatement or misappropriation of nearly $120 billion across 300 fraud cases with available information (mean of nearly $400 million per case) This compares to a mean of $25 million per sample fraud in COSO's 1999 study. While the largest frauds of the early 2000s skewed the 1998-2007 total and mean cumulative misstatement or misappropriation upward, the median fraud of $12.05 million in the present study also was nearly three times larger than the median fraud of $4.1 million in the 1999 COSO study.
- Companies allegedly engaging in financial statement fraud had median assets and revenues just under $100 million. These companies were much larger than fraud companies in the 1999 COSO study, which had median assets and revenues under $16 million.
- The SEC named the CEO and/or CFO for some level of involvement in 89 percent of the fraud cases, up from 83 percent of cases in

1987–1997. Within two years of the completion of the SEC's investigation, about 20 percent of CEOs/CFOs had been indicted and over 60 percent of those indicted were convicted.

- The most common fraud technique involved improper revenue recognition, followed by the overstatement of existing assets or capitalization of expenses. Revenue frauds accounted for over 60 percent of the cases, versus 50 percent in 1987–1997.
- Relatively few differences in board of director characteristics existed between firms engaging in fraud and similar firms not engaging in fraud. Also, in some instances, noted differences were in directions opposite of what might be expected. These results suggest the importance of research on governance processes and the interaction of various governance mechanisms.
- Twenty-six percent of the fraud firms changed auditors between the last clean financial statements and the last fraudulent financial statements, whereas only 12 percent of no-fraud firms switched auditors during that same time. Sixty percent of the fraud firms that changed auditors did so during the fraud period, while the remaining 40 percent changed in the fiscal period just before the fraud began.
- Initial news in the press of an alleged fraud resulted in an average 16.7 percent abnormal stock price decline in the two days surrounding the news announcement. In addition, news of an SEC or Department of Justice investigation resulted in an average 7.3 percent abnormal stock price decline.
- Long-term negative consequences of fraud were apparent. Companies engaged in fraud often experienced bankruptcy, delisting from a stock exchange, or material asset sales following discovery of fraud – at rates much higher than those experienced by no-fraud firms.

The term *evidence-based* is used by research analysts to describe efficacious outcomes in studies to determine the effectiveness of methodology or practice. Using the above outcomes as evidence, COSO's ICIF would be referred to as the *null hypothesis* of financial fraud or risk mitigation.[23] In the 20 years after the formation of the Treadway Commission, financial fraud was materially worse. Considering the small sample size, the results were likely gross understatements of fraud. The COSO report did not break out which public accounting firm fared worse than other firms, but the aggregated nature of the findings suggests the weakness was broad.

COSO has never published follow-up reports after the 2010 study; however, more recent headlines provide further evidence that fraudulent financial reporting has gone global.[24,25,26]

> In the 20 years that followed, after the Enron fraud faded into history, the Big Four Accounting firms rebuilt their consulting empires, advising

> on everything from insolvency to cybersecurity. But now a fresh stream of scandals has again raised concerns that firms selling services like merger advice cannot also function effectively as auditors.
>
> (Michael O'Dywer and Kaye Wiggings, London, Financial Times, "*Insurgents take on the scandal-hit Big Four*")[27]

"That has forced Deloitte, EY, KPMG and PwC to rein in the cross-selling that helped bring them a combined $157 billion in annual revenues last year – opening the door for nimble competitors to lure away star performers with generous pay cheques."

"Smaller insurgents, many of them private equity-backed, are bidding for the most lucrative divisions of the Big Four's business without the drag of the low margin, highly regulated and potentially reputation-damaging audit operations."

In an odd twist of irony, independent public accounting firms have benefited from fraud by raking in billions in consulting fees. When a company fails because of financial malfeasance, one of the other big four firms takes over to clean up the mess. Due to the lack of competition and the global reach of the largest public accounting firms, audit has become too *Big to Fail*, or has it?

COGNITIVE MAP: THE UNINTENTIONAL CONSEQUENCES OF A GLOBAL ERM FRAMEWORK

The COSO ERM integrated framework has garnered global acceptance as a standard in some circles by leveraging confusion in the public. So how did public accounting firms and internal auditors who use COSO's guidance to leverage the credibility of the five participating organizations make billions in consulting fees? We can find clues to the answer in COSO's own research.

In a research study commissioned by COSO, we can begin to see how the organization orchestrated ERM IF into an international phenomenon. The findings were presented in a 2013 Alternative Accounts Conference. The COSO board participated in a set of workshops sponsored by the Queen's School of Business and the University of New South Wales with financial support provided by the CPA-Queen's Centre for Governance. The title of the study is "Hybridized Professional Groups and Institutional Work: COSO and the Rise of Enterprise Risk Management." The authors of the report were Christie Hayne, School of Business, Goodes Hall, Queen's University, Kingston, ON, Canada, and Clinton Free, Australian School of Business, University of New South Wales, Sydney, Australia.

Excerpts from the report are presented below:

> This study specifically aims to examine the emergence and institutionalization of COSO's ERM-IF. Adopting a qualitative research design, we interviewed a range of individuals directly involved in COSO's Board and Project Advisory Council at the time the ERM-IF framework was devised, as well as the principal authors of the framework. We also interviewed individuals outside of the COSO groups (e.g., consultants, executives) that we felt would offer valuable insights into the process of diffusion. In total, we conducted 15 interviews with individuals important to COSO and the ERM-IF. We also consulted a large body of secondary materials to provide further evidence and substantiate findings.

This study makes two key contributions. First, it presents an account of the mechanisms and processes that gave rise to the formation of COSO's ERM model, which has become the dominant risk management model in North America and beyond. We detail how COSO engaged in a comprehensive project of institutional work comprised of political, cultural, and technical activities (Lawrence & Suddaby, 2006)[28]; (Corbett, Kirsch, 2001)[29], (Davila, 2009)[30], Perkmann & Spicer, 2008).[31] Drawing upon taxonomies developed in the area of institutional work, we illustrate the varied and overlapping forms of agency that enabled COSO's ERM-IF to successfully institutionalize.

Recent research in the area of institutional work augments and extends institutional theory, a perspective which has wide currency in accounting research. While others have focused on categories of institutional work (e.g., Goretzki, Strauss & Weber 2013)[32], we adopt a holistic approach to illustrate the wide ambit of work required to successfully diffuse a new managerial technology. We demonstrate that COSO's institutional work was marked by non-sequential, often serendipitous, actions that acted to overlap and reinforce each other. To the best of our knowledge, this article is the first to fully elaborate the notion of institutional work in accounting research.

Second, we present a more fully articulated conception of the actors involved in the supply side of a management innovation. Specifically, we draw attention to the notion of *hybridized professional groups*, reflecting the way that COSO was able to draw importantly from the social and cultural capital, networks, and resources of its members in disseminating the emerging model. Miller, Kurunmaki and O'Leary (2008)[33] argue that existing literature has largely neglected the hybrid practices, processes, and expertise that make possible lateral information flows and coordination across the boundaries of organizations, firms, and groups of experts or professionals.

COSO's research suggests that its ERM integrated framework did not emerge from the rigors of scientific testing or statistical analysis but instead was an orchestrated effort coordinated by its Board members who leveraged

the "cultural capital" of its five professional organizations reinforcing credibility through its members in accounting, auditing, academics, researchers, and select consultants. The actions taken by the COSO Board were deliberate efforts undergirded by the credibility of forming a nonprofit group of professional associations which grew out of the Treadway Commission. Notwithstanding the fact that its framework is not designed to withstand the rigors of a robust risk framework.

> Scarbrough (2002[34]) argues that professional groups tend to fulfill theorization roles in the shaping of a management fashion while consultants fulfill the diffusion side), we demonstrate that a more distributed but cohesive group of actors – comprised of accountants, auditors, academics, researchers, and consultants – was able to perform multiple roles and effectively support both the development and preservation of the concept.

The researchers compared the emergence of COSO's ERM to past fads in management.

> Many researchers have observed that management innovations – including ISO standards (Corbett & Kirsch, 2001)[35], product development management control systems (Davila et al., 2009)[36], activity-based costing (Malmi, 1999), total quality management[37] (Sharma et al., 2010[38]), performance-based incentives (Bol & Moers, 2010) and the balanced scorecard (Busco & Quattrone, 2009; Qu & Cooper, 2011) – have swept across a broad range of industrial sectors in the past two decades (Abrahamson & Fairchild, 1999; Alcouffe, Berland & Levant, 2008; Bort & Keiser, 2011; Jackson, 2001).
>
> The diaspora of associated entities provided a key platform for advocating and promoting the ERM technology and provided a stable and influential network of support. Our analysis suggests that, as a large, multi-faceted hybridized professional group, COSO was able to bridge conventional diffusion categories of disruption, creation, and maintenance.

This study sheds light on the deliberate steps COSO took to create a platform for commercial growth under the auspices of an independent nonprofit to reap billions in consulting fees for public accounting firms. The study is interesting in what is not included in its analysis:

(1) There is no due diligence provided on other existing risk frameworks for comparison to their own ERM IF.
(2) None of the academics or consultants provided detailed empirical evidence of the effectiveness of COSO's principles or guidance in real-life settings even though it had been in use for approximately 12 years after the Treadway Commission's report had been issued.

(3) The public accounting firms had 12 years to gather extensive data on the performance of COSO's ICIF to help inform how to extend its framework at the enterprise level and chose not to do so.
(4) If COSO had conducted such an analysis, the findings were not shared with researchers who conducted an extensive literature review in preparation for the study.
(5) Why did COSO not address the initial gap (human failures) identified in its own guidance? Extensive academic literature from Paul Slovic, Dan Kahneman, Amos Tversky, Frank Knight, Herbert Simon, and many other giants in psychology and economic theory was available to provide guidance for human behavior and decision-making under uncertainty.

Ultimately, the study was not conducted to determine if COSO's ERM integrated framework was effective in its mission. The study was designed simply to determine how effective COSO had been at creating a facade of legitimacy as a risk management framework with no efficacious outcomes from its guidance.

Many risk professionals and business executives are still surprised to learn that COSO ERM IF is not a risk standard and not required by legal mandate. COSO has been effective at "socializing" its principles as a best practice; however, COSO provides no metrics from which to measure the performance of its guidance. In other words, COSO simply filled a vacuum in risk management leadership that continues to prevail and created the appearance of a standard through the force of cohesion of its members collectively advocating for its guidance. Comments from researchers and participants on the COSO board exemplify their awareness of how confusion in organizational risk practice created opportunities for its integrated internal control framework.

> As it [COSO ERM IF] emerged, it became apparent that risk management was a canvass with a host of aspiring artists. Within the broad area of financial management, management accountants, internal auditors, external auditors, management consultants as well as a new and increasingly visible body of risk managers (see Aabo, Fraser & Simkins, 2005[39]; Hall, Mikes & Millo, 2013[40]) all sought to stake a claim as the concept opened up opportunities for applied use.
>
> In effect, this made risk management different from other innovations in accounting such as activity-based costing, the balanced scorecard or risk-based auditing, which have generally been circumscribed to particular areas of management accounting, auditing, or financial accounting. In this sense, COSO's ERM-IF is an innovation that is remarkable in its breadth (contested by a range of sub-disciplines) and commercial penetration (applied throughout the world).

> While there is no legal mandate for its use, it nevertheless has attracted normative force. While Olson and Wu (2008) claim that there are over 80 risk management standards across the globe[41], research has consistently identified COSO ERM-IF as the best known (Fraser et al., 2008) and most widely diffused risk management standard (COSO, 2010b). The institutional work that has facilitated this rise is thus an important object of scholarly attention.

COSO ERM, like other subjectively defined risk management frameworks, is a prime example of the *rational man theory,* homo economicus, at play in enterprise risk practice. Economic theory of a rational man posits that humans innately possess all the skills and capabilities to always make rational choices. Research in economic theory and behavioral science has soundly refuted the fallacy in rational man theory by pointing out obvious examples of contradictions in rational behavior expressed in contemporary society. Homo periculum (*human risks or risk wo/man*) is a play on words like *homo economicus* in economics.[42] *Homo periculum* is introduced to define the fallacy of using subjectively defined risk processes; a fallacy in judgment that an organization's subjectively defined pursuits in risk management are conducted optimally. The persistence of the fallacy in *homo economicus* continues in risk practice today leading to failed performance and expectations in risk governance. This is a cognitive risk, a blindness to heuristics and biases, that limits our ability to recognize errors in judgment. A more detailed explanation of homo periculum will follow in part 3.

The critique is not all negative. COSO was instrumental in focusing attention on the basic elements of a risk program for compliance. COSO's ICIF is foundational yet as we enter a digital age of innovation, smart systems, and hybrid work we must move forward with risk tools and technology equal to the task of a new digital operating environment. The "E" in ERM is no longer relevant. Risks are not contained by physical walls. Digital business models create digital risks that are not addressed or even contemplated in COSO's guidance.

COSO's research study also contained warnings about the dual role COSO has created as a trusted agent and an adviser on risk management. "For some, however, accounts of institutional entrepreneurship have tended to be hagiographic and represent a bridge too far in asserting the heroic influence of individual agents" (Delmestri 2006;[43] Lawrence, Suddaby and Leca 2009;[44] Suddaby 2010[45]). As Lawrence, Suddaby and Leca (2011, pp. 52–53[46]) put it:

> Missing from such grand accounts of institutions and agency are the myriad, day-to-day equivocal instances of agency that, although aimed at affecting the institutional order, represent a complex mélange of forms of agency – successful or not, simultaneously radical and conservative,

> strategic and emotional, full of compromises, and rife with unintended consequences.
>
> A wide range of studies have examined the factors that support the demand for management innovations. The phenomenon of management "fads" and "fashions" has inspired a large body of research, prompting some commentators to question whether management fashions research itself has become the next academic fad (Clark, 2004[47]). The social and organizational functions of management innovations are generally related to reducing uncertainty, insecurity, ambiguity, and imperfection (Mazza & Alvarez, 2000[48]) and providing managers with an image of innovativeness (Kieser, 1997[49]) or even heroism (Clark & Salaman 1998[50]). Somewhat paradoxically, this is often achieved through the use of concepts that are of high linguistic ambiguity. (Benders & Van Veen 2001[51])

The warnings are prophetic and capture the risk of using COSO's ERM framework to address even mundane risks. The AICPA guidance above succinctly points out the risk of untrained auditors using their own audit risk tool inappropriately. Many risk and compliance professionals erroneously believe that the process of implementing COSO's framework is an act of risk management. The goal of risk management is *actively seeking to learn what you don't know about risks*. The real nature of risk management is reductions in ignorance about risk writ large. Knowledge of a risk is the first step of discovery followed by an understanding of root cause analysis in risk origination and finally risk treatments.

Researchers in the study provided extraordinary insights from participant's comments in individual interviews. The following commentaries from board members, consultants, and academics provide an intimate perspective in how COSO ERM was conceived and promoted as a risk management framework from an insiders' perspective:

> COSO is kind of an odd organization, not just in terms of being a virtual organization but, you know, what is it? It's not really a standard setter and yet it is kind of a standard setter. It's not a company; it's not a for-profit organization. And so, I think, when COSO comes out with guidance, it carries a pretty unique credibility because you can't attribute their actions to a profit motive per se.
>
> (Douglas Prawitt, Interview 5)

The cipher COSO itself is noteworthy. Described as "disarmingly mundane" by Consultant 3, COSO leaves unspecified the identity of the involved organizations and imparts an almost faceless proceduralism to COSO's activities.

Members of the COSO Board describe how confusion in public perception in COSO's not-for-profit status creates a shield from scrutiny into public accounting firm's profit motives.

What followed from these discussions was a recognition of the failure COSO's integrated internal controls framework and the need to move on to the next approach of promoting an enterprise-wide framework to replace ICIF.

> Oliverio (2001) pointed to a number of failings including the absence of implementation guidance and clear allocations of responsibility as well as the imperative of an enterprise-wide approach. Furthermore, the competing frameworks were all motivated in some part by observations that COSO's IC-IF was no longer adequate in managing against diverse and growing risks. Where internal control was once seen as a valuable process for assuring the achievement of an organization's goals, it was seen to come under increasing scrutiny.[52]
>
> There were some people who were looking ahead and saying "Okay, what's the next step?" We [COSO] have this internal control framework out here and now companies are using it, auditors are looking at internal controls…. What's the next step in the evolution of things? What are outside parties interested in? They are interested in how you're controlling things, but what's at the core of that control framework? First, it's identifying risk and then implementing controls to mitigate and control those risks…. So, in a way, the COSO internal control framework was a rudimentary risk management framework.
>
> (Douglas Prawitt, Interview 5)

> In effect, what PwC was able to do was to position itself to roll out its framework as the international benchmark. Under the COSO badge, PwC was able to take the lead in consulting in the area.
>
> (Consultant, Interview 3)

> What the profession needed was a comprehensive way to talk about risk. There are many ways of looking at risk but what we found is that people were talking and using the same terms in different fashions and so forth. And our view was that we needed a comprehensive framework on enterprise risk management, and it had to be across the enterprise and that if we could introduce the framework, it could get more people talking about enterprise risk management-management and therefore moving to manage risk in a much more effective way. So that was the motivation behind starting with the ERM framework.
>
> (Larry Rittenberg, Interview 7)

> Because of that lack of a mandate [from a regulator, for example], organizations can sort of pick and choose pieces of it that work and not feel like they have to do a full blown implementation. We're in the early phases of ERM where people are just out there picking, there's no mandate for anything and so I think people have found it helpful, but I guess it's good that they're not being forced into it at this point. ERM is so complex to really do, companies have realized if they try to go from A to Z, it will stall.
>
> (Mark Beasley, Interview 3)

> I think part of it is because of the COSO consortium of organizations and frankly PricewaterhouseCoopers having been the author of the COSO ERM report – the names attached and the fact that COSO's internal control became a standard. The background and expertise of those organizations, and if I may say so also PwC, has caused people to look to it as the place to go in gaining insight, in gaining direction on how to build an ERM architecture in their organizations.
>
> (Rick Steinberg, Interview 9)

This is an excellent time to introduce cognitive mapping.[53] The term was generalized by some researchers, especially in the field of operations research, to refer to a kind of semantic network representing an individual's personal knowledge or schemas. The cognitive map above provides a look into the "mind's eye" of participants as they deliberate the merits of adopting COSO ERM IF.[54]

> Part of it is probably, just the fact that it's a US framework, to be honest with you. I think that carries a lot of clout, probably decreasingly so the way the world is moving, but I think that it still does carry some impact.
>
> (Douglas Prawitt, Interview 5)

> The whole US thing; it's what I call the McDonald effect: it's American, it's big, and it's what the New York Stock Exchange will accept.
>
> (John Fraser, Interview 1)

> I was invited to speak in Tokyo, and I remember talking to the Minister of Economy … he said, "But you also have to understand that many Japanese businesses are already New York Stock Exchange traded and so whatever they hear is happening in the US, they want to do it". He said, "Many others are New York Stock Exchange wannabes. So, they're not on the New York Stock Exchange yet, but they want to

> figure out what the best practices are in the US and then get ready and say that they're already doing those practices … so that division is going to implement enterprise risk management or some COSO framework to make it look more relevant."
>
> (Paul Walker, Interview 8)

> Some accounting firms were fairly responsive to it [COSO's ERM-IF] and kind of did similar to us [PwC], kind of developed methodologies and things to go deliver services around it. There was also some who felt that they could build a better mousetrap or already had a better mousetrap.
>
> (Frank Martens, Interview 14)

> Most consulting firms want to have tools and frameworks that are branded their own so they can use them, even if it's just a slight change. I think everybody tries to come up with their own little process wheel, everybody tries to come up with their own framework for looking at it, everybody tries to come up with their own common risk language, it's just the way it is.
>
> (Consultant 1, Interview 10)

> There are a lot of mouths to feed, and we were out hawking for work like everyone else. And COSO was a name that people knew … Sure most of the big players refined this to develop their own proprietorial tools, but the COSO model opened the door if you like.
>
> (Consultant 3, Interview 12)

The comments from board members, consultants, and public accountants give you a real sense of the genesis of COSO ERM. There clearly was recognition that a singular focus on internal controls was no longer sufficient and a new approach was needed. One interviewee noted, "ERM is so complex to really do." ERM is hard because the methods for analyzing disparate risks in aggregate requires different approaches than subjectively defined audit risk tools. It is unlikely that measures of "likelihood" and "impact" are sufficient analytical predictors of enterprise-wide risks such as cyber, operational, human, technological, and strategic risks in aggregate.

On the one hand, there is no longer a regulatory justification for COSO to continue to exist 36 years after the conclusion of the Treadway Commission. The Sarbanes–Oxley Act of 2002 has still not materially reduced fraudulent financial reporting. On the other hand, neither the SEC nor the Public Company Accounting Oversight Board has fully addressed the inherent conflicts of interest in the dual role of consulting and audit advisory work.

The firewalls that should exist have proven to be made of paper mâché, if they exist at all. Corporate boards and management must take back control of the audit committee's clearly defined scope to ensure audit independence. There is now a robust and thriving community of risk professionals and risk advisory firms to provide organizations with independent risk guidance or to supplement existing risk departments.

Auditors and public accounts have a value role to play in advancing internal controls over financial statements. More advanced guidance is needed on digital controls, connected devices, external third-party controls in the cloud, and on vendor site inspections. As organizations continue the transition to digital strategies, support to strengthen internal controls over financial reporting provides ample opportunity for public accounting firms to consult and advise. The SEC should also ensure and encourage an expansion of regulated public audit firms' eligibility and regulate independent risk advisory firms to enable competition for access to the global marketplace of ideas in financial accounting and risk management.

Researchers demonstrate the challenges in creating a competitive market in public accounting.[55]

Because public accounting is a regulated practice, the profession actively manages its relationship with the state. While prior studies have analyzed the profession's efforts to shape its regulatory environment, few studies have examined the profession's pointed attempts to influence a specific regulatory policy that affects the practice of auditing in the United States. Drawing on extant theories of regulation and political economy, this study investigates the rationality and effectiveness of political action committee (PAC) contributions paid to members of the US Congress by the US public accounting profession during the policy formulation period of the Sarbanes–Oxley Act of 2002.

Based on the results of empirical tests, we conclude that the US profession strategically manages its relationship with the federal government, in part, through direct involvement in the financing of political campaigns. Furthermore, the profession's pattern of contributions implies an ideologically conservative as well as a professional regulatory motivation for providing financial support to federal legislators. Thus, although the US profession continues to proclaim the primacy of its public interest orientation, it does not appear to be politically neutral when attempting to influence public policy.

DECODING THE FAILURE IN AUDIT AND CONFUSION IN ENTERPRISE RISK MANAGEMENT

The unintentional *noise* in public accounting and auditing has cost financial markets trillions of dollars in real and potential losses on a global

scale – creating a massive cognitive risk and one that could have been mitigated had Congress, the SEC, and the public understood the need to focus on the root cause of risk (human behavior) instead of internal controls over financial reporting. Herbert Simon pointed out this risk in 1947 in *Administrative Behavior* and introduced the concept of "bounded rationality."[56] Simon recognized that a theory of administration is largely a theory of human decision making, and as such must be based on both economics and on psychology.

Simon presented arguments against the then prevalent theory that "humans as agents who are consistently rational and narrowly self-interested, pursue their subjectively-defined ends optimally." Even though academics have settled the fallacy of belief in perfect rationality, remnants of these beliefs and practices still operate in corporate boards, government, and other institutions whether we consciously realize it or not. Our inability to recognize these risks is what I call cognitive risks.

Cognitive risks exist in many forms but primarily manifest in inattentional blindness to risk in judgment, bias, and impacts in human error.[57] Inattentional blindness

> occurs when an individual fails to perceive an unexpected stimulus in plain sight, purely as a result of a lack of attention rather than any vision defects or deficits. When it becomes impossible to attend to all the stimuli in a given situation, a temporary "blindness" effect can occur, as individuals fail to see unexpected but often salient objects or stimuli.

Examples include texting while driving, or decision-making while distracted by calls or deadlines. While we value multitasking, we are lousy at doing it well. Counterintuitively, inattentional blindness occurs by blindly following what other organizations have adopted as "best practice."

Why is cognitive risk relevant? Behavioral economists and researchers have already identified similar risks in heuristics, bias, health, and safety issues; however, to date, their insights have not been applied to risk governance specifically. The idea became obvious to me as an area in need of attention and research after reading the insightful examples provided in the book, *Noise*. An entirely new and unexplored approach to thinking about risk has been revealed in the precepts in *Noise*. Kahneman et al. present a simple approach, *decision audits*, to detect the presence and the magnitude of this hidden risk.

As an example, the global adoption of COSO ICIF and COSO ERM IF is noisy and biased on several fronts. Let me explain further. The process of implementing COSO ICIF is both *noisy* and *biased* in that no two organizations adopt the processes and principles in the same way. The definition of "noise" is variability (dispersion) in judgment(s). What that means in

practical terms is two-fold: a) COSO lacks a verifiable target of performance for risk mitigation when a partial implementation is as satisfactory as a full implementation. b) COSO lacks any predictive value in how effective the framework would perform as evidenced by the variability in disparate implementation outcomes.

The second major problem with COSO's two frameworks is they are biased toward a focus on internal controls over financial reporting. This point was made clear by COSO itself in the creation and explanation of the ICIF. A biased framework is systemically incorrect in that no matter the means of implementation, users will view risks in one way limiting one's view of the spectrum of risks that exist. This is a classic cognitive risk in inattentional blindness!

There are two kinds of error: *Noise and Bias*. Consider a group of friends at their favorite pub playing a game of darts. The group is made up of four teams who play every Friday night. Team 1's darts consistently hits near the bullseye. The team 1's tightly clustered darts represent a perfect pattern. Team 2 is consistently off target to the left, but also in a tightly clustered pattern of darts (*biased*). Team 3's darts are widely scattered with no discernable pattern (*noisy*), and Team 4's darts are off target but also widely scattered (*both noisy and biased*). Now convert the darts into business decisions. Bias has gotten more attention, but noise is a hidden culprit in the flaw of judgment and more than expected.

A layman's explanation may also be helpful. Here is a practical example: If two dozen firms of the same size and risk profile adopt COSO's ICIF or its ERM IF in disparate ways, there is no way to determine if COSO's framework is an effective tool to mitigate risks because of inherent noise and bias in how the framework is implemented. In practical terms, inconsistency in how COSO's framework is implemented creates a regulatory lottery. If a regulator finds deficiencies in one firm, the same deficiencies or greater may exist in other firms creating a systemic risk within the industry. The evidence of this lottery effect has played out in fraudulent financial reporting across different industries after the partial adoption of different components of COSO's two main frameworks.

Fundamentally, COSO's ICIF and its ERM IF are flawed risk frameworks and the billions spent on implementation are the costs of error in judgment. COSO's own research is evidence of inherent flaws in its framework, but the real damage in corporate governance is the expectation that COSO's framework is a best practice in risk management.

Over-reliance on subjectively defined risk management programs is an example of the fallacy I call, cognitive risk, or *homo periculum*. *Homo periculum* is a fallacy in assuming frameworks like COSO's ERM IF are optimal approaches to achieving maturity in risk management programs. Compliance-oriented frameworks are helpful to ensure consistency in institutional behavior but are only the first step in a multidisciplinary process

toward building a robust risk practice. This concept may be hard to grasp initially because many risk professionals are not familiar with the science of risk. But consider that all buildings rely on a good foundation based on ground and weather conditions the architect must consider for long-term sustainability, including maintenance and upkeep.

Or consider the analogy one senior executive frequently used. A race car needs good brakes, suspension system, and tires for different weather and road conditions to allow the race car driver to perform optimally to win while remaining safe. Weakness in any of the foundational areas of design create inherent vulnerability to the entire system. That is why the World Trade Center towers held after the planes hit allowing most of the participants to escape unharmed versus the catastrophic failure of the Condo towers on the beach in Florida. Attention to details matter because the details allow you to take informed risks after you have addressed the fundamentals.

Risk management is not solely about following someone else's script for what a risk program is, it is about understanding the proper design of a risk program to address your unique and specific risk needs.

Reimagining the organization is about designing new solutions for the needs of your firm not following the leader, especially when the self-anointed leaders know less about your risks than you do.

The merging of psychology and economics has resulted in a more robust understanding of judgment and decision-making under uncertainty and helps explain why this flaw has gone undetected and underrepresented in traditional risk frameworks like COSO ERM, ISO 31000, and most existing risk programs. It is premature to call any traditional risk framework "mature" without an extensive grounding in the science of risk whose root and branch is informed in psychology, behavioral economics, behavioral science, and decision science. Economists dubbed the rational man theory "homo economicus." I have dubbed the rational risk theory in traditional risk practice "homo periculum," a fallacy I call cognitive risk, a fallacy that organizations' subjectively defined pursuit of risk management is conducted optimally.

The noise in public accounting and audit that I referred to earlier is the same as those referenced in the prologue: "wherever there is judgment, there is noise – and more of it than you think" (*Noise*, p.12, Kahneman, Sibony, and Sunstein 2021). Public accounting and audit are predicated on judgment. Judgment is required in response to accounting for the complexity of today's business environment. A problem arises when attempting to overly rely on subjective judgment in the application of complex risk analysis without appropriate rules-based guidance.

We now know that noise is the variability of judgment. When business leaders and auditors differ on "the risk" of a course of action or the outcome of certain business practices, these disagreements create bias and noise in judgment. When organizations lack the tools to minimize bias and

noise, the resulting residual risk is costly whether known or not. This risk is largely undetected until the accumulation of these unresolved judgments add up to an unexpected failure or operational inefficiencies.

Now that we have established the context for why corporate failure and fraud continues to grow unabated, let us turn our attention to other examples of failure in case studies to demonstrate how cognitive risk thrives in a variety of circumstances.

NOTES

1. https://www.cbsnews.com/news/great-resignation-60-minutes-2022-01-10/.
2. https://www.cnbc.com/2022/01/14/the-great-resignation-expert-shares-the-biggest-work-trends-of-2022.html.
3. https://en.wikipedia.org/wiki/Committee_of_Sponsoring_Organizations_of_the_Treadway_Commission.
4. https://www.sec.gov/news/speech/1989/012689grundfest.pdf.
5. https://www.sec.gov/rules/final/33-8238.htm.
6. https://www.justice.gov/criminal-fraud/foreign-corrupt-practices-act.
7. See COSO, "Internal Control-Integrated Framework" (1992) ("COSO Report"). In 1994, COSO published an addendum to the Reporting to External Parties volume of the COSO Report. The addendum discusses the issue of, and provides a vehicle for, expanding the scope of a public management report on internal control to address additional controls pertaining to safeguarding of assets. In 1996, COSO issued a supplement to its original framework to address the application of internal control over financial derivative activities.
8. https://www.academia.edu/45682001/The_Future_of_Risk_Management.
9. https://corporatefinanceinstitute.com/resources/knowledge/other/top-accounting-scandals/.
10. https://www.sec.gov/rules/final/33-8238.htm.
11. https://www.aicpa.org/resources/download/aicpa-audit-risk-assessment-tool.
12. https://www.sec.gov/info/accountants/audit042707.htm.
13. https://www.sec.gov/info/accountants/audit042707.htm.
14. https://www.telegraph.co.uk/business/2022/01/12/kpmg-auditor-uses-minority-ethnicity-defence-forged-carillion/.
15. https://corporatefinanceinstitute.com/resources/knowledge/other/top-accounting-scandals/.
16. https://www.coso.org/documents/FraudStudyOverview_000.pdf.
17. https://en.wikipedia.org/wiki/Committee_of_Sponsoring_Organizations_of_the_Treadway_Commission.
18. https://en.wikipedia.org/wiki/Committee_of_Sponsoring_Organizations_of_the_Treadway_Commission.
19. https://corporatefinanceinstitute.com/resources/knowledge/finance/financial-engineering/.
20. http://guide.berkeley.edu/graduate/degree-programs/financial-engineering/.
21. https://erm.ncsu.edu/library/article/coso-fraud-study/.
22. https://pcaobus.org/oversight/inspections/firm-inspection-reports.

23. https://en.wikipedia.org/wiki/Null_hypothesis.
24. https://amp.ft.com/content/a8c60322-3e56-4889-b346-e34d3c5f1e97.
25. https://www.ft.com/content/57e0ff80-de17-48b1-9da7-5bdbaaad8898.
26. https://amp-ft-com.cdn.ampproject.org/c/s/amp.ft.com/content/548f99ff-1815-4af1-a7ef-e631cf9c720a.
27. https://www.ft.com/content/57e0ff80-de17-48b1-9da7-5bdbaaad8898.
28. T. Lawrence and R. Suddaby (2006), Institutions and institutional work, in: S. Clegg, C. Hardy, W. Nord, and T. Lawrence, eds., *Handbook of Organization Studies*, London: Sage, 215–254. https://doi.org/10.4135/9781848608030.n7.
29. C.J. Corbett and Kirsch, D.A., INTERNATIONAL DIFFUSION OF ISO 14000 CERTIFICATION, 05 January 2009, https://doi.org/10.1111/j.1937-5956.2001.tb00378.x
30. Davila, et al, framework 48, Management Control Systems and Open, pps. 55-59.
31. M. Perkmann and A. Spicer (2008). How are management fashions institutionalized? The role of institutional work. *Human Relations*, 61(6), 811–844. https://doi.org/10.1177/0018726708092406
32. L. Goretzki, E. Strauss, and J. Weber (2013), An institutional perspective on the changes in management accountants' professional role, *Management Accounting Research*, 24(1), 41–63.
33. P. Miller, L. Kurunmaki, and T. O'Leary (2008), Accounting, hybrids and the management of risk, *Accounting Organization and Society*, 1 October. https://doi.org/10.1016/J.AOS.2007.02.05.
34. H. Scarbrough (2002). The role of intermediary groups in shaping management fashion: The case of knowledge management. *International Studies of Management and Organization*, 32(4), 87-103.
35. C. J. Corbett and D. A. Kirsch (2009), International diffusion of ISO 14000 certification, *Operations Management*, 5 January 2009. https://doi.org/10.1111/j.1937-5956.2001.tb00378.x.
36. Y. Lievens, W. van den Bogaert, and K. Kesteloot (2003), Activity-based costing: A practical model for cost calculation in radiotherapy, *International Journal of Radiation Oncology, Biology, Physics*, 57(2), 522–535. https://doi.org/10.1016/s0360-3016(03)00579-0. PMID: 12957266.
37. Teemu Malmi (1999), Activity-based costing diffusion across organizations: An exploratory empirical analysis of Finnish firms, *Accounting, Organizations and Society*, 24(8), 649–672, ISSN 0361-3682. https://doi.org/10.1016/S0361-3682(99)00011-2, https://www.sciencedirect.com/science/article/pii/S0361368299000112.
38. S. D. Levitt, J. A. List, and S. Sadoff.
39. Tom Aabo, John R. S. Fraser, and Betty J. Simkins (2005), The rise and evolution of the chief risk officer: Enterprise risk management at hydro one, *Journal of Applied Corporate Finance*, 17(3), 62–75, Available at SSRN: https://ssrn.com/abstract=622744.
40. Matthew Hall, Anette Mikes, and Yuval Millo (2013), How do risk managers become influential?: A field study in two financial institutions, Revision, 2013 October 17.
41. Indeed, several international risk management standards pre-date the COSO framework including CAN/CSA-Q850-97: *Risk Management: Guideline for Decision*-Makers issued by the Canadian Standards Association in 1997 (62

pages); BS 6079-3:2000 *Project Management: Guide to the Management of Business-related Project Risk* issued by the British Standards Institution in 2000 (22 pages); JIS Q2001: 2001(E) *Guidelines for Development and Importance of Risk Management* Systems issued by the Japanese Standards Association in 2001 (20 pages); IEEE Standard 1540-2001: *Standard for Software Life Cycle Processes – Risk Management Standard for Software Life Cycle Processes – Risk Management* issued by the American Institute of Electrical and Electronic Engineers in 2001 (24 pages); and AS/NZS 4360:2004: *Risk Management* issued jointly by Standards Australia/ Standards New Zealand in 2004 (24 pages). Based on a wide-ranging analysis of several standards, Raz and Hillson (2005) conclude that there is "wide consensus regarding the main steps and activities of a generic risk management process" (p. 65) and that "where there are apparent differences in process, these are largely attributable to variations in terminology" (p. 64).

42. https://en.wikipedia.org/wiki/Homo_economicus.
43. G. Delmestri (2006), Streams of inconsistent institutional influences: Middle managers as carries of multiple identities, *Human Relations*, 59(11), 1515–1541.
44. T. B. Lawrence, R. Suddaby and B. Leca (2009), Introduction: Theorizing and studying institutional work, in: T. B. Lawrence, R. Suddaby, and B. Leca, eds., *Institutional Work: Actors and Agency in Institutional Studies of Organizations*, Cambridge: Cambridge University Press. https://doi.org/10.1017/CBO9780511596605.
45. R. Suddaby (2010), Construct clarity in theories of management and organization, *Academy of Management Review*, 35(3), 346–357.
46. T. Lawrence, R. Suddaby, and B. Leca (2011), Institutional work: Refocusing institutional studies of organization, *Journal of Management Inquiry*, 20(I), 52–58. Sagepub.com/journal/Permissions.nav. https://doi.org/10.1177/1056492610387222.
47. T. Clark (2004), The fashion of management fashion: A surge too far? *Organization*. https://en.wikipedia.org/wiki/Homo_economicus.
48. C. Mazza and J. L. Alvarez (2000), Haute couture and Prêt-à-Porter: The popular press and the diffusion of management practices, *Organization Studies*, 21, 567–588. http://dx.doi.org/10.1177/0170840600213004.
49. A. Kieser (1997), Rhetoric and myth in management fashion, *Organization*, 4(1), 49–74. https://doi.org/10.1177/135050849741004.
50. Timothy Adrian Robert Clark and Graeme Salaman (1998), Creating the 'right' impression: Towards a dramaturgy of management consultancy, *Service Industries Journal*, 18(1), 18–38. Research Collection Lee Kong Chian School of Business. Available at: https://ink.library.smu.edu.sg/lkcsb_research/6284.
51. Jos Benders and Kees Van VeenView all authors and affiliations 8(1). https://doi.org/10.1177/135050840181.
52. Clark, T. (2004). The fashion of management fashion: A surge too far? Organization, 11(2), 297-306.
53. Simon Ungar (2005), Cognitive maps, in: Roger W. Caves, ed., *Encyclopedia of the City,* Abingdon; New York: Routledge, 79. https://doi.org/10.4324/9780203484234. ISBN 9780415252256. OCLC 55948158.

54. https://en.wikipedia.org/wiki/Cognitive_map.
55. https://www.researchgate.net/publication/223239550_Money_politics_and_the_regulation_of_public_accounting_services_Evidence_from_the_Sarbanes-Oxley_Act_of_2002.
56. https://en.wikipedia.org/wiki/Herbert_A._Simon.
57. https://en.wikipedia.org/wiki/Inattentional_blindness.

Corporate Defense and the Value Preservation Imperative

Bulletproof Your Corporate Defense Program

Sean Lyons

CRC Press
Taylor & Francis Group
AN AUERBACH BOOK

Corporate Defense and the Value Preservation Imperative

Bulletproof Your Corporate Defense Program

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Printed on acid-free paper
Version Date: 20160510

International Standard Book Number-13: 978-1-4987-4228-3 (Hardback)

Library of Congress Cataloging-in-Publication Data

Names: Lyons, Sean (Sean Gilbert), 1966- author.
Title: Corporate defense and the value preservation imperative : bulletproof your corporate defense program / Sean Lyons.
Description: Boca Raton, FL : CRC Press, 2017. | Series: Internal audit and IT audit series | Includes bibliographical references and index.
Identifiers: LCCN 2016013712 | ISBN 9781498742283 (alk. paper)
Subjects: LCSH: Corporate image. | Corporate culture. | Corporations--Public relations. | Corporations--Investor relations. | Corporations--Valuation.
Classification: LCC HD59.2 .L96 2017 | DDC 659.2--dc23
LC record available at https://lccn.loc.gov/2016013712

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the CRC Press Web site at
http://www.crcpress.com

Contents

SECTION II A Tactical Perspective

SECTION III An Operational Perspective

SECTION IV An Integrated Perspective

Preface

VALUE PRESERVATION AND CORPORATE DEFENSE

Stakeholders naturally expect successful organizations to deliver sustainable value over the long term. In the aftermath of the financial crisis and ongoing corporate scandals, many stakeholder groups are now questioning the adequacy of the measures currently being undertaken by organizations to safeguard and preserve stakeholder value. Not surprisingly it is common for postmortem investigations into the causes of corporate scandals to typically identify deficiencies and weaknesses in the corporate defense program of the organization(s) concerned. These deficiencies and weaknesses can begin with the nonexistence of a corporate defense program; however, individual corporate defense issues can also vary considerably. Typically, examples of these issues can include failures in corporate governance, poor risk management, compliance failures, unreliable intelligence, inadequate security, insufficient resilience, ineffective controls, and the failures by assurance providers. The existence of more than one of these issues in any given organization tends to exacerbate the initial problem and can eventually result in exponential collateral damage to stakeholder value. When these types of issues become systemic within an industry or business sector, it will very often result in some form of a broader crisis within that industry or sector, and, in some cases, this will spill over into the broader economy.

Logically, if deficiencies and weaknesses in corporate defense programs tend to result in corporate losses and failures, then improved corporate defense programs will help better safeguard against the occurrence of such scenarios. What is needed is effective corporate defense rather than corporate defense theater. This requires the design and implementation of more robust corporate defense programs that will help to not only safeguard stakeholder interests but also to optimize stakeholder value.

ABOUT THIS BOOK

This is the first book on the market to finally address the umbrella term *corporate defense*, and to explain how an integrated corporate defense program can help address an organization's value preservation imperative. For the first time, the reader is provided with a complete picture of how corporate defense operates all the way from the boardroom to the frontlines. It provides comprehensive guidance on how to implement an integrated corporate defense program by addressing this challenge from strategic, tactical, and operational perspectives. This arrangement provides readers with a holistic view of corporate defense. It enables readers to fully understand and appreciate an organization's value preservation imperative and the resulting requirement to deliver a robust corporate defense program. It addresses the corporate defense requirement from various perspectives and helps readers to understand the critical interconnections and interdependencies that exist at strategic, tactical, and operational levels. It facilitates the reader in comprehending the importance of appropriately prioritizing corporate defense at a strategic level, while also educating the reader in the importance of managing corporate defense at a tactical level, and executing corporate defense activities at an operational level.

THE PURPOSE OF THIS BOOK

With the above in mind, the purpose of this book is therefore threefold. First, the focus of this book is on recognizing that delivering long-term sustainably requires both a focus on value creation and a focus on value preservation. Second, this book is intended to help to clarify the ongoing obligation

on organizations to take adequate measures to preserve stakeholder value and to be able to demonstrate that they are taking appropriate actions to safeguard stakeholder interests. Third, this book is designed to help provide a comprehensive roadmap or blueprint for readers on how best to deliver a world-class corporate defense program in order to successfully achieve the value preservation imperative. This includes preserving existing value and preventing unnecessary losses.

THE BOOK LAYOUT

This book is divided into four sections and is designed to provide the reader with a comprehensive understanding of corporate defense from top to bottom. Certain sections may however be of a greater interest to readers with relevant experience in that particular area.

Section I—A Strategic Perspective: The strategic section will initially be of utmost interest to readers who are on board level or in executive management positions. From a strategic perspective, this section addresses the requirement for an organization to consider a balance between both short-term value creation and long-term value preservation as part of its business strategy. At a strategic level, this requires a corporate defense strategy that is in alignment with the overall business strategy.

Section II—A Tactical Perspective: The tactical section will initially be of utmost interest to readers who are in C-suite or middle-management positions. From a tactical perspective, it addresses the organization's need to design a comprehensive corporate defense framework that enables the alignment, integration, and management of the organization's corporate defense-related activities (i.e., governance, risk, compliance, intelligence, security, resilience, controls, and assurance). This section also considers the specific aspects of the individual corporate defense-related activities in some detail.

Section III—An Operational Perspective: The operational section will initially be of utmost interest to the readers who are in business line management positions or to those who are directly involved in the execution of corporate defense-related activities. From an operational perspective, it addresses the management and execution of the corporate defense program and considers the main challenges facing the implementation of such a program. It also considers the requirement to continuously monitor and report on the status of its ongoing progress.

Section IV—An Integrated Perspective: The integrated section should be of interest to all readers irrespective of their position, experience, or background. From an integrated perspective, it addresses the value proposition associated with an effective corporate defense program. This section helps to outline the business case for such an effective corporate defense program by addressing its potential positive contribution at strategic, tactical, and operational levels.

Although certain sections may stimulate individual readers more than others depending on their background knowledge and experience, it is ultimately envisaged that the book will help each reader to develop a more rounded and holistic view of corporate defense and will provide them with a comprehensive understanding of the workings of corporate defense at all levels.

Sean Lyons

ACKNOWLEDGMENTS

I thank Dan Swanson for encouraging me to write this book in the first instance and for his support and insightful feedback on the original manuscript. I also acknowledge Igor Lamser of the RiskCenter, David Honour of the Business Continuity and Resilience Journal, and Matteo Tonello of the Conference Board for being supportive of my work on corporate defense at its early stages and for helping to bring it to the attention of a wider audience. I would also like to acknowledge the following organizations for their invitations to speak to their members on corporate defense at different stages over the past 10 years: the Asian Confederation of Institute of Internal Auditors (ACIIA), the Professional Risk Managers' International Association (PRMIA), the Society of Actuaries (SOA), the Business Continuity Institute (BCI), ASIS International, the Intangible Asset Finance Society (IAFS), and the MIT Club of Portugal.

I especially acknowledge the input of Ross Coakley in helping to develop a visual representation of the corporate defense management (CDM) framework, in creating many of the images for this book, and for modeling the YouTube video entitled "Corporate Defense Management (CDM): A Multi-dimensional Framework." On a personal level, Ross was my very first friend and has remained a lifelong friend over the past five decades. His incredible scientific mind and his generous and helpful nature mean that his presence and company is always a very rewarding experience. Ross's positive attitude, bravery, and courage in dealing with his recent motor neuron disease (MND) diagnosis are an inspiration to all who know him. Thank you for all your help and I wish you well my dear friend.

I thank my mother Eileen and all my family and friends for their encouragement and support on this journey. Last but by no means least, I would like to dedicate this book to my late father, Michael Lyons.

Author

Sean Lyons is globally recognized as a corporate defense thought leader and strategist. He is acknowledged as the pioneer responsible for proposing the umbrella term *corporate defense* to represent an organization's collective program for self-defense, and also for being the first to propose the extended *five lines of defense* oversight model that is currently receiving increasing levels of regulatory attention. Sean has published internationally, and has spoken as a subject matter expert at lectures, seminars, and conferences in Europe, North America, and Asia. These speaking engagements include topics such as corporate governance, enterprise risk management (ERM), compliance, security, business continuity, internal controls, assurance, and governance, risk and compliance (GRC). His work on corporate defense has been cited in a number of books and a multitude of other publications on the above topics. As the architect of the cross-functional discipline of CDM, he is widely regarded as the foremost authority in this emerging field. With more than 20 years of experience in corporate defense activities, he is a firm advocate of the requirement for corporate defense to play a more prominent role in corporate strategy. In an effort to help achieve this objective, Sean has been an active contributor to public consultations in many of the above topics.

In 2015, Sean was a member of the Editorial Advisory Board of the inaugural publication of the *Journal of Enterprise Risk Management*, the first academic journal to focus solely on enterprise risk management. In 2013, he was the invited keynote speaker at the Asian Confederation of Institute of Internal Auditors (ACIIA) Chief Audit Executive Leadership Forum in Mumbai, for their two-day conference entitled, "Enterprise Defense Management: Internal Auditors to the Fore" (a theme that was based on his CDM framework). In 2011, he was an invited member of the taskforce of the International Corporate Governance Network (ICGN) on promoting the ICGN *Corporate Risk Oversight Guidelines*. In 2010, the conference board published his influential paper entitled, "Security as a Critical Component of Corporate Defense" that was sponsored by the U.S. Department of Homeland Security (DHS) as part of their ongoing project to assess security risk exposure and business preparedness in the private sector. Sean was shortlisted as a finalist in the GRC MVP 2009 Awards run by the U.S.-based GRC Group (SOX Institute), which was cochaired by Senator Paul Sarbanes and Congressman Michael Oxley. These awards recognized individual achievements and professional contributions in governance, risk management, and compliance, and honored professionals who demonstrated excellence in this field. For a number of years, Sean was also the resident contributor in the field of corporate defense for the RiskCenter, a New York financial risk management media company (then based on the Wall Street).

Selected publications of his work are presently available for download online at http://ssrn.com/author=904765.

Section I

A Strategic Perspective

1 Business Strategy and Value Preservation

The superior man, when resting in safety, does not forget that danger may come.*

Confucius

1.1 CORPORATE STRATEGY IN AN ERA SEEKING SUSTAINABLE SUCCESS

So far the twenty-first century has already seen a litany of corporate failures and financial scandals that have had a significant impact on the reputation of the corporate world, and perhaps more tellingly on broader society. The early part of this century highlighted the dangers of excessive optimism with the boom and bust of the dotcom bubble, and it also identified continued weaknesses and deficiencies in corporate behavior resulting in the demise of corporate giants such as WorldCom, Enron, and Arthur Anderson. At the time such events were heralded as valuable lessons and served as warnings for future generations. Less than a decade later, the dangers of excessive optimism were again highlighted, this time by the occurrence of what is now commonly referred to as the great financial crisis that affected the planet on a global scale and its impact is still being felt in many geographic regions (UNCTAD 2010).

These events have clearly shaped how society, in general, now views the corporate world and indeed how it views the working of capitalism and the capitalist system. As a consequence, stakeholders all over the world are now placing increased pressure on organizations to focus on their stakeholder obligations, with a view to delivering sustainable value to stakeholders in the long term. This has resulted in more and more organizations recognizing their obligations in this regard, and

* Per *The Best Confucius Quotes*, April 2015, James Alexander, Crombie Jardine Publishing Ltd, Bath, UK.

many are now duly focusing their attention on the concept of sustainability and the delivery of long-term stakeholder value.

There now appears to be an increasing recognition that any such long-term obligation can only be delivered once the concept of sustainability in its broadest sense has been successfully incorporated into how the organization does its business. This means that long-term sustainability must be embedded into the organization's vision and become a common feature of consideration at strategic, tactical, and operational levels within the organization itself. It means addressing it within the corporate strategy.

Traditionally, the concept of corporate strategy was considered to be concerned with helping to ensure that the organization was capable of providing sustainable above average industry performance, thereby allowing it to perpetually deliver superior returns and help create wealth for its shareholders. The global financial crisis however clearly exposed systemic weaknesses in the prevailing corporate strategy on an international scale. The subsequent fallout from this seismic event has resulted in the reputation of the corporate world being severely tarnished in the eyes of many stakeholders. The resulting negative impact has been felt not only by shareholders but also by management, staff, clients, business partners, suppliers, regulators, local communities, and indeed society in general, who all have eventually suffered as a consequence of flawed corporate strategies.

The corporate world now faces multiple pressures to reform the manner in which business is conducted and how individual organizations are managed. Stakeholders are now demanding higher standards of corporate citizenship in terms of integrity, ethics, and accountability. They are also demanding an improved strategic direction in order to provide them with greater protection and assurance going forward. Increasing pressure in the form of proxy advisor demands and pressure from stakeholder activist groups have prompted a rigorous search for an improved approach to corporate strategy, one that is aimed at helping organizations to foster an age of long-term sustainability.

1.1.1 Corporate Strategy: A High-Level Perspective

Corporate strategy is typically concerned with the overall scope and direction of an organization's strategic activities. It is concerned with the *big picture*, the complete strategic scope of the enterprise, and how its various business activities operate together in order to help achieve particular strategic goals and objectives. Corporate strategy is commonly used to help develop a long-term plan for a company's success, the main purpose being to help ensure that the business can outlast the competition over the long term, regardless of the type of internal or external conditions that may present themselves. It is regarded as the roadmap to be followed by the organization and can also impact on its culture and be a driver of corporate behavior.

1.1.1.1 The Strategic Agenda

Corporate strategy will be dictated by the organization's strategic agenda. Typically, the board of directors set an organization's strategic agenda after giving due consideration to the relevant organizational conditions. The strategic agenda should be set to address the organization's aspirations in relation to issues such as growth, performance, and change. The board, in association with the executive management, should provide the vision and leadership required to determine the appropriate path that they consider will best deliver on the organization's aspirations over time.

An organization's aspirations should represent a reflection of its culture and the expectations of the organization as a whole. Corporate culture is commonly referred to as *the smell of the place* or *how things are done around here*. An organization's culture reflects the common shared values and ideals that are embedded within the organization. Values include the beliefs that are shared throughout the organization. They drive culture and strongly influence the behaviors, actions, and decisions of the board, management, and staff. The organization's aspirations are reflected in its sense of *raison d'être*, its aim, its reason for being. Its aspirations reflect the purpose of the organization, its ambitions, and the planned journey ahead. This journey ahead is best understood and described in the organization's vision and mission statements.

1.1.1.2 Vision and Mission Statement

The requirement for a vision and mission statement is aptly described in the following words by the late Warren Bennis, an influential authority on leadership, when he said: "To choose a direction, an executive must have developed a mental image of the possible and desirable future state of the organization. This image, which we call a vision, may be as vague as a dream or as precise as a goal or a mission statement" (Hindle 2008).

The vision: Ideally the corporate vision should help to immediately visualize the *big picture* by providing a description of the organization's desired future state. It represents a broad, forward-thinking image that the organization should have for its purpose and intentions before it sets out to achieve its goals and objectives. Typically a corporate vision should be short and succinct, and represent an inspiring image of its mindset and aspirations. It should describe where the organization wishes to go and what it is trying to create and develop. Ultimately it should describe what it intends to achieve in the future and should represent a source of motivation for the workforce.

Mission statement: A mission statement should typically be more detailed than the corporate vision and represent a statement of rationale regarding the fundamental purpose of the organization. It should help guide the decisions and actions of the organization and it is therefore important that it is stated clearly so that it is understood by all, and can serve as a constant reminder to its stakeholders of the purpose of the organization's existence. It can be used as a reference point to evaluate the current activities or to help resolve trade-offs or disputes between different stakeholders. The mission statement should broadly outline the aims of the organization and what unique contribution the organization provides to its stakeholders. The lack of a clear mission statement diminishes the organization's ability to verify that it is progressing on its intended course.

The vision and mission statements help provide a background to the organization's strategic objectives for the future, without specifying the measures that need to be taken to help achieve the desired goals. In this way, they help to provide a context within which the organization's strategy can be formulated.

1.1.1.3 Managing Corporate Strategy

The clearer the organization's vision and mission statement, the easier it is for the strategic management of the organization to clearly oversee the setting and implementation of its corporate strategy. The corporate strategy represents a statement of strategic intent for the organization by way of strategic objectives. The strategy itself should be based on the principal findings of the strategic assessment conducted by the organization's strategic management. It should clearly outline the strategic choices that have been made and the rationale supporting these choices. Corporate strategy refers to the highest business strategy of the organization. It should address the mix of markets the organization intends to compete in and the way in which the strategic network should be coordinated and integrated.

The board of directors and the executive management team are expected to bring considerable professional experience and diversified business insight to their contribution on the organization's corporate strategy. Their sound judgment, specialist knowledge, and leadership qualities will be of particular benefit when deciding on which services, products, and markets to compete, and in which geographic regions to operate. Management of the corporate strategy process typically involves a number of basic phases.

Strategy formulation: The corporate strategy is in effect the path that has been chosen in order to arrive at the end vision. It therefore represents the roadmap by which the organization intends to complete its mission. A clear formulation of the corporate strategy should help the board and executive management to connect the ideas, assumptions, and decisions that are driving the organization's strategic agenda. It should help to provide a definite plan of

action going forward to achieve this end. In determining corporate strategy, due consideration should be given to matching the organization's strategic activities to the organization's environment, its available resources (e.g., people, processes, and technology), and the extent of its capabilities. Due consideration should also be given to the values the organization wishes to espouse and the expectations to be set for its various stakeholders. The strategy formulation process should help set the organization's strategic objectives and help to identify and select an appropriate business model. It should clearly state the organization's strategic goals and outline the strategic measures and initiatives required to achieve these objectives. These strategic goals should be tangible and achievable in order to be helpful in guiding all of the organization's business activities going forward.

Strategic planning: Corporate strategy is typically implemented via a strategic plan; however, there are many examples of organizations whose failure was attributed to its inability to successfully execute its strategy in practice. Successful strategy implementation requires a carefully planned approach, a very high level of discipline, and involves the effective implementation of critical business activities in order to make it work. It is unreasonable to expect the attainment of strategic goals without the adherence to a carefully planned approach and the implementation of the required tasks. The strategic planning process should consider the corporate culture, the resources available to the organization, and the projected timescales required to achieve the stated strategic objectives. The strategic plan should guide and direct the subsequent tactical and operational planning exercises, in order to help ensure that these plans are in alignment with the organization's strategic objectives. The resulting plans should identify tasks that are specific and measureable and will noticeably contribute toward the achievement of the strategic objectives. Many strategies fail due to poor or inadequate planning, and the quality of the final plans is generally a reflection of the quality of the planning process.

Strategy execution: Once a clear strategic plan has been formulated, the executive management is then responsible for ensuring the effective and efficient implementation of that corporate plan. Execution of the corporate strategy via implementation of the strategic plan is critical to success and should never be underestimated as it is never guaranteed. Indeed, many strategic commentators suggest that execution is the key to competitive success, as making the plan work can be an even bigger challenge than formulating strategy, or creating a strategic plan. There are many factors that can hinder successful execution, including internal politics, resistance to change, and the occurrence of hazard events. Execution involves putting the plan into action by translating planned tasks and activities into the completion of verifiable actions. It involves the effective performance of the necessary tasks outlined in the plans and this requires considerable organization, and employing resource management and change management practices. This is perhaps best achieved using a top-down approach that incorporates the full chain of command so that the required action steps are performed at strategic, tactical, and operational levels. The executive management team needs to collaborate with the line management to help ensure timely, effective, and efficient performance of the required tasks.

Strategy review: Once a strategy is executed according to the plan, there is a reasonable expectation that it will prove to be successful; however, a successful outcome can never be assumed or taken for granted as there is *many a slip between the cup and lip.* The strategy needs to be a living breathing concept that needs to be continuously monitored and assessed. The success or failure of a corporate strategy cannot be adequately assessed without a process to review how well the strategy is performing in practice. This should involve comparing the actual results against the benchmark of intended milestones and outcomes. A strategy review process represents an evaluation of the corporate strategy and substrategies, and an appraisal of the execution of the strategic plan. The process of strategy review is equally as important as the processes of strategy formulation, strategy planning, and strategy execution as it evaluates the logic and rationale of the original strategy and appraises the effectiveness

and efficiency of the implementation of this strategy. It enables the organization to focus on the appropriateness of the current strategy and to question the soundness of previous assumptions, which may no longer stand up to scrutiny due to changing circumstances and the dynamic environment of the twenty-first century. It allows an organization to re-evaluate the validity of the previous strategic choices and the extent to which ongoing performance has helped achieve the desired results. It also allows an organization to measure the variance that exists between the original desired results and the organization's actual results.

In certain cases, a strategy may prove to be successful from the very beginning, and the organization may be prepared to ratify it and endorse it going forward. In other cases, it may be determined that there is a considerable room for improvement and that the existing strategy needs to be modified or adjusted accordingly. The extent of this modification will need to be considered on the back of the results of the strategy review. In certain scenarios, the results may indicate that a serious corrective action is required. In such cases, the existing strategy may be rejected as a failure, and it may be determined that a new strategy is required and needs to be formulated.

1.1.2 Short-, Medium-, and Long-Term Orientations

An old Chinese proverb states that *a journey of a thousand miles begins with a single step* and so it is with corporate strategy. When considering the topic of corporate strategy, it is important to bear in mind that although an organization's vision may reside in the distant future, the corporate strategy should present a roadmap that will guide the organization toward the achievement of this long-term vision. This involves not only clearly identifying the organization's long-term strategic objectives, but also setting achievable strategic goals in the medium and short terms. Ideally short- and medium-term goals should be aligned to long-term strategic objectives so that the achievement of short- and medium-term goals act as stepping stones to the accomplishment of the longer-term strategic objectives, and in the process, fulfilling the organization's mission statement and ultimately realizing its corporate vision.

1.1.2.1 Short- or Long-Term View: A Sprint or a Marathon?

Although the adoption of a long-term focus in order to realize the corporate vision is indeed a worthy ambition, in the modern world it has to be acknowledged that a short-term focus is necessary in order to ensure immediate day-to-day survival. Short-term gains are required in order to achieve a long-term growth; however, excessive short-terms gains can sometimes lead to the detriment of the long-term growth and stability. It must, however, be accepted that to be successful in the long term, an organization also needs to have a certain degree of short-term success.

In the wake of the great financial crisis, many economic commentators are of the opinion that the world's financial markets are somewhat addicted to the short-term view, which in turn leads to an unhealthy obsession with the achievement of monthly revenue targets and quarterly earnings. In this light, short-sighted remuneration and compensation structures also often intensify this obsession. In fact, there is a prevailing notion that during the build-up to the global financial crisis, the business world in general became preoccupied with the pursuit of short-term gains and lost sight of the long-term bigger picture. This resulted in the development of what are often referred to as *strategic blind spots* that were later to negatively impact on wider society, both economically and socially.

1.1.2.2 The Way Forward

What is required is a balanced view whereby the organization has a clear understanding that there is no disconnect between an organization's present and future, so that they are intrinsically connected and do not exist in a vacuum. First, however, there needs to be an acknowledgment that short-term gains can indeed result in a long-term gain; however, excessive short-term gains can in fact result in a long-term pain. It must also be acknowledged that, in some cases, short-term pain is required in

order to achieve a long-term gain; however, excessive short-term pain can in and of itself also lead to a long-term pain.

This acknowledgment can help an organization appreciate that what is required is a blended approach, where one eye is focused on the medium to long-term horizon and the other eye is focused on addressing short-term issues that need to be handled in the present. Although sustainability is generally associated with the long term, its achievement requires focusing on the short-, medium-, and long-term horizons, and an appreciation that there are times when short-term instant gratification is required to be sacrificed in order to help ensure longer-term gratification.

1.2 CORPORATE STRATEGY AND VALUE CREATION

Although one organization's vision and mission statement may differ considerably from that of another, generally speaking, the vision and mission statements are concerned with contributing value to the organization's primary stakeholders. Corporate strategy is subsequently concerned with actually delivering this value to these stakeholders over the short, medium, and long terms.

1.2.1 The Value Concept in Corporate Strategy

The concept of value is an inherent aspect of the twenty-first century capitalism. The promise of value is therefore an integral part of any corporate strategy, and addressing this value proposition is an essential element of corporate strategy. Developing a value proposition is based on a review and analysis of the benefits that can be delivered by the organization to its stakeholders, less the associated costs. The residual balance represents the value proposition to its stakeholders. In order to address the value proposition, it is important to clearly understand the concept of value.

It is said that value is like beauty, as it is *in the eye of the beholder*, and it is often equated with a sense of worth that in turn can act as an incentive to take a desired action. The notion of value is increasingly being measured in both quantitative and qualitative terms in order to reflect both its tangible and intangible nature. Value may have different meanings in different contexts and to different stakeholders in terms of intrinsic as well as extrinsic value. In the final analysis, an organization's understanding of stakeholder value is best determined through engagement with its stakeholders.

1.2.1.1 Business Value as a Strategic Concept

In the realms of strategic management, the term business value is perhaps a somewhat informal concept, without any agreed consensus. The term is generally used to include various forms of value that can help determine the corporate health of an organization. More recently, the term business value is being expanded beyond the traditional, financial, and economic value to also encompass numerous other forms of perceived value. Although historically the notion of value was predominantly associated with monetary contribution, not all forms of value are directly measured in pure monetary terms and a broader notion is now emerging.

As well as value that may be quantified in financial terms, value may also manifest itself in what is described as utility value. Utility value represents the qualitative aspect of value, and it reflects value as perceived in the minds of stakeholders such as consumers and users through its capacity to meet individual human needs. Utility value is therefore recognizable by its demand and in business it is realized through its consumption.

Value in the broader sense is therefore increasingly based on its worth to the stakeholder and the stakeholder's assessment of its worth. Stakeholder value may not necessarily be assessed from a single source such as its monetary benefit, but may also be assessed in terms of what it can provide to the stakeholder and how it can help the stakeholder to achieve their various objectives. Value may therefore be measured in terms of physical, emotional, and intellectual stimulation. Consequently, the value of a product or service and the price of a product or service are not necessarily one and the same thing. In the famous words of Warren Buffett, "Price is what you pay. Value is what you get."

Business value therefore can embrace both tangible and intangible assets such as the organization's balance sheet value and the value associated with its business model and other intellectual capital. Indeed, the concept of business value can also embrace the theory that an organization's value can best be viewed as a network of relationships with stakeholders who are both internal and external to the organization itself. In this context, business value is concerned with the value embedded in these relationships over time.

1.2.1.2 Value Delivery and Realization

In business, value needs to be considered in terms of the value delivered to the various stakeholders of the organization. Value delivery refers to how the organization provides benefits to its stakeholders in the short, medium, and long terms. Organizations are concerned with questions such as *what benefits are we providing, how are we providing these benefits, and who are we providing these benefits to?* Follow-on questions may include *how can we improve on our delivery of value?* Value delivery can therefore be considered to be a source of potential competitive advantage.

Value realization on the other hand can refer to the organization's own return on its investment (financial or otherwise). Value realization involves putting in place the appropriate set of activities that are required to help ensure the expected delivery of value. The objective is to ensure that the full projected value is attained within the expected timescales. Hence the realization of value is a critical element of any successful corporate strategy. For example, once value realization starts to occur in the form of increases in cash flows, profitability, net worth, and so on, additional strategic options may begin to present themselves. Such options can include the opportunity of further growth through acquisitions, newfound interests from potential capital partners, additional strategic alliance opportunities, and enhanced exit strategies. Each organization must clearly establish its own value realization metrics in order to monitor the process effectively.

From a shareholder perspective, value may be realized through annual dividend income, or via an attractive sale or other liquidity event that provides the opportunity to transform equity into cash or other valuable liquid assets. This may involve taking-up options, or the sale of stock or other assets in the organization, whether in whole or in part, at a value that is determined by the market, which may be in excess of the shareholders' initial investment, and thereby yielding a healthy return on that investment. Other stakeholders may realize value in nonfinancial ways such as through corporate social responsibility and environmental initiatives. Over time, the organization's capacity to realize sustainable value for its stakeholders is a function of the organization's ability to create and preserve value on an ongoing basis.

1.2.2 The Value Creation Focus

What does the term value creation mean? The International Integrated Reporting Council (IIRC) describes the value creation process as follows: "Value is created through an organization's business model, which takes inputs from the capitals and transforms them through business activities and interactions to produce outputs and outcomes that, over the short, medium and long term, create or destroy value for the organization, its stakeholders, society and the environment" (IIRC 2013a). An organization can therefore create value over time through conducting a wide range of business activities that in turn produce outputs. These activities can occur within the many different environments in which the organization operates, both internal and external to the organization itself. This involves developing and managing relationships with its key stakeholders* with whom it interacts, and on whom it depends for its survival. Value can be maximized by fulfilling the needs of these key stakeholders while also considering the interests of society in general and the impact on the environment. The extent to which these needs and interests are addressed will determine the type of value that is created.

* The nature of the stakeholder relationship is addressed in Chapter 3, Section 3.3.3.

1.2.2.1 The Business Model

An organization's business model describes how the organization intends to go about creating value for its stakeholders. The business model lies at the core of an organization, and its long-term success will be determined by the resilience of its business model over time. An organization's chosen business model represents its business approach and the fundamentals of its business processes and key business activities. It reflects its system of inputs and outputs that in turn lead to outcomes that create value and help the organization to achieve its goals and objectives, and help to fulfill its mission statement in the longer term.

Organizations that operate in a number of different market segments may employ more than one business model; however, due consideration needs to be applied to appreciating the level of interconnectivity that exists between these business models and their business activities. The business model typically includes addressing a number of issues.

Key business activities: The business model should clearly identify and outline the key business activities that the organization intends to operate. Generally an organization's key business activities involve the processes by which the organization intends to convert its inputs to outputs. These outputs generally take the form of either products or services that can provide value to the organization's key stakeholders. When considering its business model, the organization should clarify how it intends to differentiate itself in the marketplace in terms of such issues as its unique selling point (USP) (e.g., product differentiation, market segmentation, supply chain, and distribution channels) to be used to deliver its products or services to its stakeholders. It should focus on how the organization intends to convey its message to its key stakeholders and how it intends to communicate with them on an ongoing basis.

The inputs: The essence of the business model is the conversion of inputs into outputs in order to create value. The business model should clearly identify and outline the key inputs required by the organization, which when applied through the business process will convert into value-added outputs. These key inputs represent those ingredients that the organization depends on in order to deliver value. The performance of its business activities provides the organization with its source of differentiation by converting its key inputs from raw materials into its finished end product. Key inputs are derived from various types of capital whereby business activities draw on many types of capital in one form or another as inputs into the value creation process. The key inputs and how they relate to the various capitals from which they are derived represent a critical aspect of the organization's business model. How the corporate strategy links key inputs to capitals, opportunities, risk, and financial performance is critical to the success of the strategy.

The capitals: The business model should clearly identify and outline the types of capitals the organization depends on for its success. Organizations typically depend on different types of capital whether they are considered tangible or intangible capitals. There is no currently universal agreement on the different types of capitals, and they may be classified in different ways by different organizations. One example is the six types of capitals identified by the IIRC as follows: *financial capital, manufactured capital, intellectual capital, human capital, social and relationship capital, and natural capital* (IIRC 2013b). These capitals represent stores of values in various forms that become inputs into the organization's business model. Such capitals can be used to release value in the form of producing outputs and outcomes when they interact and are combined, transformed, and leveraged through an organization's business process. Value is therefore created by the resulting increase, decrease, or transformation of the capitals.

The overall stock of the value stores, which is provided by the capitals, is not fixed over time, but rather they are in a continuous state of flux as they are increased, decreased, or transformed through the activities and outputs of the organization. Consequently such

interactions can in fact enhance, modify, or otherwise affect the overall capital stock. Although in theory the organization's aim is to create value in its capitals, in practice this may also involve the depletion or destruction of the value stored in some capitals while at the same time increasing it in others. In general, this can result in an overall net increase or decrease in the overall stock of the capitals.

Ultimately whether the net effect is perceived as either an increase or decrease may well depend on the perspective of the stakeholder concerned. In many instances, returns in financial capital may be dependent on interrelationships among other forms of capital in which stakeholders have different interests, for example, society and the environment. Also, not all of the capitals required by the organization are necessarily owned by that organization. Certain capitals may be the property of the organization, whereas certain others may be owned, belong to, or be an entitlement of various other stakeholder groups who in turn share in both the value created and their associated costs.

As noted earlier, there are different types of capital that organizations typically depend on for their success; however, not all organizations are equally dependent on the same capitals; therefore, different capitals will have different relevance to different organizations. Although it is likely that most organizations will interact with all of the capitals mentioned earlier, to a certain degree, some of these interactions may be considered immaterial in terms of the organization's business model.

Whether certain capitals are increasing or decreasing can affect the availability, quality, and affordability of those capitals. This is a particular issue of concern for capitals of which there is a limited supply, and capitals that are not possible to be renewed. It is important to bear in mind that the availability and supply of certain capitals can be seriously impacted by the extent to which organizations, both collectively and individually, interact with these capitals. Ultimately, such issues can in turn have a serious impact on the long-term viability of an organization's business model.

Innovation: The business model should clearly identify and outline the organization's USP over that of its competition. An organization's long-term success or failure may well be determined by how the organization addresses the age-old requirement to be innovative. The business model should clearly address the organization's attitude to innovation and its approach to responding to change. The flexibility of its strategy, the agility of the business model, and the organization's capacity and capability in adapting to change can have a profound impact on the organization's long-term viability. This may be of particular relevance when faced with sourcing inputs and capitals, and adapting business activities. Logically, the key to a long-term success lies in the extent to which the organization can foster an innovative mindset throughout the enterprise so that it becomes embedded in the corporate culture and is continually present in day-to-day activities.

1.2.2.2 The Value Creation Process

The concept of value creation lies at the very heart of corporate strategy and the business model. The value creation process itself involves initially taking the business inputs and putting them through the business model in order to eventually produce desired benefits in the form of business outputs and outcomes at the other end of the process. This process can involve applying the organization's business processes in order to combine or transform the organization's capitals, thus producing both positive and negative effects on these capitals with the intended result of the creation of value for the organization and its key stakeholders. The nature of those effects will determine the extent of the value created and the outcomes for the different stakeholder groups.

Generally speaking, value can be created over short-, medium-, and long-term time horizons, and it can be created through the use of different capitals and created for different stakeholder groups. Creating value will often involve a trade-off between the effect on different capitals, some positive

and some negative. Such a trade-off should consider the effects both individually and collectively. Assessing the nature of the value created involves considering the nature of the interdependences that exist between the capitals and their relationships with the various stakeholder groups. It is doubtful that long-term sustainable value can be created by solely focusing on increasing one individual capital at the expense of all of the other capitals. The value creation process is typically concerned with a number of issues.

Value drivers: The value creation process is concerned with determining the organization's value drivers. Typically it is the organization's value drivers that distinguish it from its competitors as they have a critical role to play in the organization's ability to create value over the short, medium, and long terms. Value drivers can vary by types of business; they can be generic, industry specific, or organizational specific and their range can vary from one organization to another. They reflect certain key elements, characteristics, or attributes that make an organization attractive to its stakeholders. Such elements consist of those unique activities, capabilities, and core competencies that enable an organization to provide a perceived competitive advantage in the perception of its stakeholders.

Value drivers may be tangible or intangible as both can contribute to the creation of value by an organization. They may reflect tangible assets owned by the organization or intangible assets that help to increase the overall desirability of the organization in the eyes of its stakeholders. In the twenty-first century, intangible assets are now increasingly being perceived as primary value drivers. Value drivers reflect those factors that are identified as having the most significant impact on the future value of the organization and those factors that can be most effectively managed and controlled. Therefore identifying and managing value drivers can help an organization to focus its attention on the key activities that are most likely to help in achieving its short-, medium-, and long-term goals and objectives.

Outputs and outcomes: The value creation process is concerned with determining the organization's required outputs and preferred outcomes. From a value creation perspective, there is a subtle but important distinction between an *output* and an *outcome*. The organization's business model represents a series of processes and activities that convert inputs to outputs. As outputs tend to be process driven, they therefore refer to planned deliverables whereby the end product typically tends to be tangible in nature and therefore can be accurately anticipated in advance, and precisely and objectively measured in quantitative terms on completion.

Outcomes, on the other hand, refer to the impact that the outputs may have on the stakeholders, both internal and external. Stakeholder reaction is typically reflected by its impact on the organization's capitals. Outcomes therefore relate to the ultimate payoff, the value added to the stakeholder as a direct or indirect result of the outputs. Therefore outputs have an impact on outcomes, but it is important to appreciate that they are not the same thing. As outcomes tend to be reaction driven, they are by their very nature less predictable than outputs and hence more difficult to anticipate as they can take place over multiple time frames.

Although an outcome may be less predictable, it is still measureable in terms of its impact (financial and nonfinancial) on the organization's capitals. This measurement may be more subjective and qualitative when dealing with nonfinancial capitals. Although outcomes can result in the anticipated, planned, or intended consequence of an output, it must also be understood that it can also result in an unanticipated, unplanned, or unintended consequence. As an outcome represents the occurrence of a change in circumstance for a stakeholder, which is a result of targeted outputs, it is important to understand that such a change can have either positive or negative consequences, which means that an outcome can present either a potential upside or a potential downside for the stakeholder and in turn the organization itself.

Although the traditional corporate strategy and the setting of strategic objectives have been primarily concerned with focusing the potential upside and intended positive outcomes, an emerging

contemporary view focuses on an appreciation that corporate strategy must also include a sufficient focus on the potential downside and unintended negative outcomes. A balanced corporate strategy should therefore incorporate a degree of both value creation and value preservation.

1.3 DEFENSE OF THE REALM: THE VALUE PRESERVATION IMPERATIVE

In business as in many other aspects of life, the reality is that the nature of uncertainty means that an organization's activities can either have a positive or a negative impact on the value it delivers to its stakeholders. Over a prolonged period of time, this value experience may include numerous fluctuations as a result of both positive impacts and negative impacts. Successful organizations however depend on their ability to both create and sustain value over the short, medium, and long terms. Over the long term, value is compounded by both creating and preserving value.

Once an organization has succeeded in creating value, it then faces the dual challenge of continuing to create value on an ongoing basis while simultaneously ensuring that it can also preserve the value that is created. Therefore, a focus on value creation alone is not considered to be sufficient, it must be accompanied by a focus on value preservation. In any event, successful organizations learn to continuously monitor the dynamics between value creation and value preservation. Unfortunately in many unsuccessful organizations, although value creation quite rightly received due consideration in corporate strategy, there is far less evidence to suggest that value preservation received a similar consideration. In general, it would appear that the requirement to preserve value is much less appreciated and therefore is often neglected.

1.3.1 The Concept of Value Preservation

What precisely is meant by the concept of value preservation? If on the one hand value creation is primarily concerned with delivering a potential upside, then on the other hand value preservation is primarily concerned with protecting against a potential downside. Indeed, there are some who would argue that *a dollar of value preserved is indeed a dollar of value created.* Logically organizations that exhibit an ability to preserve the value they have created over an extended period of time tend to be successful, whereas organizations that are unable to preserve their value tend to fall by the wayside. An inability to successfully preserve value will inevitably result in a decline in, or destruction of, value. The value preservation concept therefore lies at the heart of lasting sustainability.

The value preservation imperative represents an organization's obligation to its stakeholders to take adequate steps to preserve value. It represents the measures (formal or otherwise) taken by an organization to defend itself and the interests of its stakeholders from a multitude of potential

hazards (i.e., risks, threats, and vulnerabilities), the occurrence of which could be detrimental to the achievement of the organization's objectives. To successfully deliver on this obligation, an organization requires an appropriate program for self-defense.

1.3.1.1 The Threat of Value Reduction and Destruction

In business, organizations are constantly faced with the threat of value reduction, and often it is the extent of any value reduction that can determine the organization's ultimate fate. The existence of such a threat is simply the reality of doing business. The root cause of such threats can vary considerably, as can their timing and scale. Ultimately there are an unlimited number of events or series of events that can occur over the short, medium, and long term, which can result in the reduction or destruction of stakeholder value. Protecting and defending against the loss of stakeholder value is the kernel of the value preservation imperative. This includes an obligation to take adequate steps to anticipate, prevent, detect, and react to hazard events in order to avoid, mitigate, and manage any potential exposure in a timely manner. Although the extent to which an organization was expected to fulfill this obligation may once have been perceived as somewhat optional, this is no longer the case as it is now considered a business imperative whereby stakeholders expect and demand increasingly higher levels of due diligence in this regard.

1.3.1.2 Value Erosion, Depletion, and Decline

Organizations need to be wary that value can decline in a number of ways, ranging from its sudden depletion as a result of an unexpected liability, its gradual erosion over time due to an outdated or inflexible business model, or its complete destruction due to flawed strategic assumptions. Without taking adequate steps to help preserve value, stakeholders of the organization may find their value being eroded and the organization may find its value declining year on year. Such a decline in value can be witnessed in many different ways, all of which can result in a negative impact for stakeholders either directly or indirectly. For example, it can be witnessed in decreasing market shares, decreasing revenues, increasing costs, decreasing assets, increasing liabilities, lower profits, higher losses, lower share prices, and lower market capitalization.

1.3.2 The Corporate Defense Necessity*

In order to help preserve value, organizations are now expected to take steps to protect stakeholder value, and the protection of stakeholder value is synonymous with corporate defense-related practices such as corporate governance, risk management, and compliance activities. Such practices are considered necessary to help defend stakeholder value against the vagaries of any potential threats that could result in value reduction or destruction. In the eyes of an increasing number of stakeholders, once value has been created, it then needs to be protected and defended.

The cost associated with defending stakeholder value was traditionally considered to be part of the inherent costs of doing business; however, more enlightened organizations are no longer regarding this as a cost but rather as an investment in the organization's own long-term sustainability. This suggests that corporate defense-related practices can also represent an opportunity for the organization to create a competitive advantage in the form of security over stakeholder value. It is anticipated by some that such stakeholder value security will in time attract a premium that will be factored into future stakeholder value calculations.

1.3.2.1 Defending and Safeguarding Stakeholder Interests

The calculation of stakeholder value involves an assessment of the extent to which stakeholder value is being optimized, and this can include the extent to which stakeholder interests are being

* Failure by an organization to recognize this necessity will be seen by many stakeholders as representing a strategic "Red Flag".

safeguarded. In other words, there is an expectation that organizations are not only working toward adding to, or increasing stakeholder value, but also taking measures to protect the existing stakeholder value from decline. For example, shareholders expect the organization to take measures to help protect the organization's share price and its market capitalization.

In the twenty-first century, stakeholders are now demanding at least reasonable levels of due diligence in this regard and are increasingly prepared to hold the organization to account should they be considered negligent in their efforts. At a minimum, there is now an expectation that the organization will take all appropriate measures to ensure that it has adequate corporate defense initiatives in place. Organizations are expected to at least be able to provide reasonable comfort that stakeholder value will not be diminished.

1.3.2.2 The Necessity for Improved Corporate Defense Measures

In the build-up to the financial crisis, there were clear signs that stakeholder interests were not being adequately defended (Lyons 2006a), and the subsequent fallout from the related global economic recession has highlighted common weaknesses and deficiencies in relation to organizations' corporate defense activities. Ongoing events continually expose how so many organizations in various business sectors all over the world have failed to adequately defend the interests of their multiple stakeholders. This has resulted in the reputation of the corporate sector being severely tarnished in the eyes of many stakeholders.

Numerous national and international reviews have clearly highlighted the general failure to fully appreciate and consider the potential threat to stakeholder value as a core issue. Many of these reviews identified weaknesses and deficiencies in corporate defense-related activities as having a significant contribution to the occurrence of this economic downturn and have particularly identified areas such as failures in corporate governance and the management of risk and compliance as major contributory factors: "We conclude that dramatic failures of corporate governance and risk management at many systematically important financial institutions were a key cause of this crisis" (FCIC 2011). As a result, numerous stakeholder groups are now demanding improvements in the corporate defense-related measures employed by their organizations to defend their interests. These improvements need to start at a strategic level, beginning with looking at how the value preservation imperative is addressed when setting the corporate strategy.

1.3.3 Reimagining Corporate Strategy

Historically, when setting strategy, business organizations have tended to treat the critical issues of value creation and value preservation as separate issues. In retrospect, given the nature of their symbiotic relationship, this has proven to be both an artificial and dangerous segregation. Although, in general, corporate strategy does tend to formally address the issue of how the organization intends to create its value, the equally important issue of how the organization intends to preserve its value generally does not form part of corporate strategy. A similar observation very often applies to the foundations of the organization's business model. The result has been a clear distinction between the overall corporate strategy and a corporate defense substrategy, as generally speaking the strategic echelons of the organization tend to consider the issue of corporate defense as somewhat peripheral to corporate strategy and the business model. Consequently the board and executive management tend to approach corporate defense-related matters with extreme caution because they do not understand how corporate defense fits with corporate strategy. In fact, corporate defense matters can tend to become relegated so far down the strategic priority list that their relevance becomes difficult to establish. In extreme situations, those involved in corporate defense activities can feel as if they are regarded as almost like second-class citizens within the organization. In such circumstances, corporate defense practices can become disengaged from core business activities, and can very often exist in silo-type environments, whereby they operate as an afterthought to core business activities. This type of attitude simply cannot be allowed to continue;

things have to change, and going forward the corporate defense strategy needs to be considered as an essential element of the overall corporate strategy.

1.3.3.1 Re-Examine the Way We Do Business

In many organizations, what is now required is a fundamental re-examination of how their business is conducted. This will involve a serious reframing of how they currently view the creation and preservation of value in the context of their corporate strategy and business model. They will need to redefine not only how their corporate strategy but also how the foundations of their business model address the corporate defense conundrum. Their business fundamentals need to formally incorporate the requirement for an adequate corporate defense strategy in order to help ensure value preservation and facilitate the build-up of business value over time.

Logically it is much more difficult to build-up significant business value over time if while creating new value, existing value is being depleted or destroyed at the same time. It is important that going forward when an organization addresses the challenge of defending stakeholder value within its corporate strategy and that this is clearly stated in terms of strategic objectives and clearly identified as a strategic activity within its business model. Indeed, prudence would suggest that a sustainable corporate strategy and business model should balance the organization's desire to increase its value over time, with the stakeholder desire to defend the value that has already been realized. Long-term sustainable success requires the two to go hand-in-hand, a concept that needs to be embedded throughout the organization, and across all of its business activities. An appreciation of how an organization needs to address defending its stakeholder value has far reaching implications at strategic, tactical, and operational levels and presents interesting challenges for the organization itself.

1.3.3.2 Corporate Defense Is No Longer Considered Optional

To establish a sustainable strategy and business model, an organization needs to actively and systematically embed corporate defense-related practices at the strategic, tactical, and operational levels. Embedding the corporate defense concept into an organization's DNA requires a basic acknowledgment from the very top to the very bottom of the organization that good corporate defense represents a business imperative, rather than some sort of prerogative or optional add-on. Redefining strategy and the business model to incorporate the appropriate mix between the focus on increasing value and defending value will have significant implications for the organization and all of its stakeholders.

1.4 STRIKING A BALANCE BETWEEN OFFENSE AND DEFENSE

Military to civilian transition.

An old sporting aphorism states that *offense wins games, defense wins championships*. In business speak, offense refers to the focus on bringing the dollar in through the front door, whereas defense refers to the focus on preventing the dollar from leaving through the back door (Lyons 2014). In other words, in the corporate world, offensive activities are associated with the organization's focus on upside rewards, whereas defensive activities are associated with the organization's focus on the prevention of downside loss. What is essential is finding the correct balance between taking larger risks and reaping larger rewards. If organizations in the twenty-first century are to deliver long-term sustainable value, they must learn to achieve a healthy balance between their focus on offense and their focus on defense. Getting this balance right can help provide better opportunities for delivering long-term sustainable value.

A commonly held view of economic theory is that the Western capitalist model is primarily driven by the motivating factors of greed and fear. The former is the motivation to extend ourselves in search of even greater rewards, whereas the latter is the motivation to protect what has already been achieved lest it should be taken from us. Progress no doubt requires both, whereas prudence and common sense would suggest that long-term sustainability requires a healthy blending of the two.

Unfortunately the search for balance, or the middle path, is not a new concept and is one that goes back thousands of years. In the Western philosophy, especially that of the Greek philosopher Aristotle, the *golden mean* represented the desirable middle between two extremes, one of excess, the other of deficiency. Another famous Greek philosopher Socrates taught that man "must know how to choose the mean and avoid the extremes on either side, as far as possible." The search for balance continues to this day.

1.4.1 The Tao of Corporate Defense

In the Eastern philosophy, the Taoist tradition places great emphasis on the search for harmony between opposing extremes or forces. Taoism refers to the concept of the *yin* and *yang,* which is used to describe how seemingly opposing forces are inherently interconnected and interdependent in the natural world. Each of these forces is present within the other and in turn gives rise to the other. There are many examples of natural dualities such as dark and light, night and day, female and male, wet and dry, and action and inaction that are cast as yin and yang in the Taoist thought. In the corporate context, perhaps the duality of offense and defense can best be understood and appreciated when viewed in this context.

1.4.1.1 Offense and Defense Viewed as Yin and Yang

Viewing offense and defense in terms of the Taoist duality can help provide a higher level of insight into this complex relationship. Offense (yin) and defense (yang) are considered to be antagonistic yet complementary principles that fit together seamlessly. They represent opposites that are bound together and intertwined, and are capable of working together in a perfect harmony. Offense and defense are considered to be the two halves within a greater whole and together they complete a unifying circle. Their relationship is not static as every aspect of business has both offense and defense aspects, and these continuously interact and never exist in a stationary state as the balance ebbs and flows. It is therefore impossible to talk about offense or defense without a reference to the opposite, as offense and defense are rooted together and one cannot survive without the other. It is therefore important that they are not separated or addressed in isolation.

In essence, offense and defense actually transform each another, as each contains a portion of the other within it. Offense contains within it the potential for defense, and defense contains within it the potential for offense. They are finely balanced in a dynamic equilibrium, whereby a deficiency in one can unbalance their relationship, and if one disappears the other is very likely to follow. In short, when either offensive or defensive activities become the subordinate, the whole is likely to suffer eventually.

Unfortunately, in the business world, this is rarely immediately apparent because offense elements are clear and obvious, whereas defense elements are more hidden and subtle. Therefore extremes in offense are far more regular than extremes in defense, although this can also occur. Ultimately, however, extremes in either offense or defense can result in the development of an organization that is putting its long-term sustainability in jeopardy.

1.4.2 The Current Strategic Imbalance

Unfortunately, the financial crisis and indeed more recent corporate scandals continue to clearly highlight the imbalance that currently exists between offense and defense in the corporate mind-set. Recent events indicate that short-termism tends to focus disproportionately on the former, often neglecting the latter. Such a mind-set has resulted in excessive risk taking in search of short-term rewards at the expense of longer-term sustainability.

There were many reasons for the financial crisis, and the following strategic, tactical, and operational issues have strongly contributed to the unhealthy imbalance referred to earlier (Lyons 2012a):

- An overly narrow focus on pure financial metrics while ignoring important nonfinancial issues
- A focus on short-term interests at the expense of broader, long-term stakeholder interests
- The lack of board-level appreciation of the necessity of having a formal, systematic *corporate defense program* in place within their organization to help ensure that their stakeholder interests are adequately safeguarded
- The lack of a seat at the C-suite table for a *defense champion* to challenge, scrutinize, and add a degree of balance to the formulation of corporate strategy and policies
- The resulting lack of transparency and responsibility for corporate defense where accountability is fragmented and diluted at the executive management level
- The lack of coherent coordination of defense-related activities at a functional level, leading to the development of silo-type structures that are not in alignment with one another but rather operate in isolation, resulting in both ineffectiveness and inefficiency

Although a great deal of work has been undertaken since the financial crisis to improve corporate behavior, there is sufficient evidence available to suggest that many of these issues still need to be addressed as weaknesses and deficiencies in corporate defense activities remain commonplace. Examples include the rogue trader Jerome Kerviel at Societe Generale, the cyber theft at SONY, the health and safety issues in the clothing industry in Bangladesh, and more recently the Volkswagen emissions scandal, to name but a few. This will require a notable correction to the current imbalance in order to create a natural harmony between offense and defense.

1.4.2.1 Achieving a Healthy Balance

The challenge facing organizations is wide ranging; however, restoring a natural equilibrium between offense and defense in the corporate mind-set will go a long way toward improving the situation going forward. This requires joined-up thinking and perhaps can best be achieved by a degree of tweaking and joining of the existing dots, rather than by a complete overhaul of the entire system.

Correction of this current imbalance requires a broader stakeholder (shareholders, clients, staff, business partners, local communities, and society) focus and a more holistic view of how best to safeguard these stakeholder interests in the long term. Ensuring that there is a sufficient focus on long-term sustainability (i.e., survival) will require a subtle shift in corporate consciousness. Such a shift will necessitate a change of attitude in relation to the fundamentals of corporate health and a clear appreciation of corporate health requirements in the short, medium, and long terms. This will involve further educating the corporate world so that defensive behavior can be seen in a positive

light and as being necessary for the achievement of long-term sustainability, rather than being seen as a necessary evil. Corporate defense is not about business prevention; it is about doing the right business in the right way.

In far too many organizations there is a defense deficit. Corporate defense is more likely to be implied in corporate strategy rather than being considered a core element of business strategy, and more often than not there is an absence of any formal corporate defense strategy. Corporate strategy must therefore incorporate a balance between offense and defense in order to arrive at a natural equilibrium. This will require a subtle blending of these antagonistic yet complementary principles that are inherently intertwined and mutually interdependent within a dynamic system. In essence, the principles of offense and defense represent two sides of the same coin, and therefore cannot and should not be addressed in isolation from one another.