Cyber Security and Business Resilience

Thinking strategically

The cyber threat landscape

For today's organisations, which rely heavily on technology, and particularly the Internet, to do business, cyber attacks are a very real threat. Worse, the cyber threat landscape is complex and constantly changing. For every vulnerability fixed, another pops up, ripe for exploitation.

Attackers are often motivated by a very high risk-to-reward ratio: digital information is easy to copy, and it can be hard for a victim to detect that an attack happened at all, let alone figure out who was behind it. Furthermore, technology enables attackers to target anyone, anywhere, from the comfort of their home, often using automated tools to identify their victims – and their vulnerabilities.

Committing crimes over the Internet can also be very lucrative. Unlike stealing physical credit cards, which tend to be blocked very quickly, digitally targeting someone gives an attacker the chance to steal that person's identity and get credit cards issued in the victim's name. The victim would likely only become aware of the theft after checking their bank statements or receiving a phone call from the bank. Upscale that by targeting businesses that hold databases with thousands or even millions of credit card details and personal information about their owners, and the profits will certainly be far greater than those of a physical crime conducted in the same timescale and with the same manpower.

Because virtually every organisation holds valuable information, often in huge quantities, everyone is a target. It should therefore not come as a surprise that 46% of UK businesses experienced at least one cyber attack or breach during 2019, which increased to as much as 75% for large businesses.[1] Those may include attacks like simple phishing emails, but even the most basic attack, if executed successfully, can wreak havoc if you are not prepared.

Clearly, it is in your organisation's best interests to protect itself and invest in cyber security. This paper will look at some of the most important, high-level points you should consider when planning your cyber security – and business resilience – strategy.

What exactly is cyber security?

Cyber security is concerned with securing your information assets and systems on three fronts:

1. **Confidentiality**
   Information assets and systems should only be accessible to those who need access to them.
2. **Integrity**
   Information assets and systems should be protected from unauthorised modification, destruction and loss.
3. **Availability**
   Information assets and systems should be accessible to authorised persons as and when necessary.

Considering all three aspects, also referred to as 'CIA', means that you will not make the common mistake of only taking confidentiality into account. Clearly, restricting information on a need-to-know basis is a critical element of security, but that information is only useful if you know it is correct and you are able to access it when you need it.

Making trade-offs

There are no two ways about this: security requires trade-offs. Some solutions are more expensive than others, but might be easier to implement. Others might be cheaper, but require a bigger sacrifice in convenience or privacy. There are solutions that only reduce the impact or likelihood of an incident, and others that achieve both.

Ultimately, security is all about considering those trade-offs, and deciding which are worth making. It is about determining your needs and making sensible decisions about how to meet them without making unpalatable sacrifices. Clearly, budget is a factor, but so are time, resources, convenience, flexibility and privacy. At the end of the day, no security solution is perfect or foolproof, but making strategic decisions can make the trade-offs worth the cost, financial or otherwise.

Building resilience

Unfortunately, even the most secure organisation can still fall victim to a cyber attack. To a large extent, it is simply a case of having the odds stacked against you: while you need to protect all your assets from all types of threat, an attacker requires only one weakness to get into your systems. On top of that, any security measure you put in place is only designed to stop a handful of threats – at most. That means that it is likely to be inherently ineffective against other kinds of threat.

It is important to both recognise these challenges and not view them as insurmountable.

To understand why the former is so important, you only have to look at the past. History teaches us that if you assume something cannot go wrong, you may find it difficult, if not impossible, to remedy the situation if things do go awry. The Germans in World War II deemed their Enigma machine uncrackable, so never even considered the possibility that the British were intercepting and decrypting their messages. The RMS *Titanic* was deemed unsinkable, so only had 20 lifeboats with capacity for just over 1,000 people, when the ship itself could carry more than 3,000 individuals.

With this in mind, acknowledging that your security system may fail despite your best efforts enables you to pre-emptively consider how something might go wrong and what you can do to limit the damage in such a situation. The consequences of an attack – no matter how rare – can be crippling if you have not planned how you will respond, but thinking resiliently will enable you to recover.

However, understanding the need for cyber resilience and the broad strokes to implementing it is not enough. Any strategic approach, no matter how mature or sophisticated you intend your defences to be, must begin with a risk assessment.

Risk assessment

Conducting a risk assessment is a critical part of identifying what cyber security measures you need to implement and to what degree, keeping your defences cost-effective and sustainable.

A large part of any risk assessment should be identifying your threats and vulnerabilities. The key questions are who might attack you, how they would go about it, and what their motivations are. Who might target your line of business? What data do you hold? Who might want that data (and is prepared to commit a crime in order to obtain it)? What methods are they likely to use? For each attack type, what and where are your weak points?

To answer such questions, it helps to have a clear idea of exactly what incidents you are trying to prevent. Everyone wants to avoid adverse consequences, but the incidents that can specifically damage *your* organisation operationally, financially and/or reputationally are unique. The information you hold is not the only asset you need to protect – there are also, for example, critical business processes that you must seek to preserve, and websites that need to stay live.

Furthermore, not all information is equal in value and, to make matters more complicated, the same information may have a value that changes over time – information about new products and services, for instance, is far more valuable when not yet available in the public domain. Your regulatory or contractual requirements, like those imposed by the General Data Protection Regulation (GDPR) and Data Protection Act (DPA) 2018, may also inform your priorities.

After you have identified your risks, you should respond to them in one of the following ways:

- **Treat** – implementing one or more measures to reduce the likelihood and/or impact of the risk.
- **Transfer** – e.g. through insurance or outsourcing.
- **Terminate** – eliminating the source of the threat.
- **Tolerate** – actively choosing to retain the risk, e.g. because it is not possible or too expensive to treat the risk, or because the risk is deemed acceptable.

Defence in depth

No single measure works 100% of the time. As such, a treated risk is still a risk, albeit one that is less likely to occur and/or less harmful if it does. Even if your measures are effectively implemented and well-maintained, security can still fail. Therefore, a more dynamic approach, where individual security measures work together effectively and make up for each other's weaknesses, is required.

In a defence-in-depth approach, you have multiple, layered defences in place so that, if one layer fails, the other layers still prevent the attack from succeeding. Ideally, each layer also presents a different challenge for an attacker (think moats and walls for castles).

The concept is as applicable to physical security as cyber security. When defending against malware, for example, your primary goal is to stop it from entering your networks, so your first layer of defence will consist of measures like whitelisting and firewalls. Your next layer might aim to prevent malicious code from executing, while a further layer might assume that the code has already been executed and attempts to contain it from spreading further via measures like network segmentation and segregation.

When considering your options in respect of defence in depth, the key is to consider how your controls might be circumvented. That often requires you to locate the weakest link in your security, which a smart attacker will find and attempt to exploit. In other words, the strength of your overall security system is equal to the strength of your weakest point. If you want to improve overall security to mitigate the risk, you must find and strengthen your weakest link. Be aware, however, that this is no easy task, if only because it will depend on the threat – who is the attacker and what are their intentions?

As a complement to defence in depth, you can make use of 'choke points', whereby you force traffic (whether people or data) into a smaller channel that is easier to secure, as you can focus your resources. If you know where your weak points are, you also know where to look for intruders.

Prevention

Prevention starts with steps that are characteristic of a risk assessment. First, you need to know what assets you are trying to protect. From there, you can determine how those assets might be compromised (vulnerabilities), and who or what may compromise them (threats).

Keep in mind that not every threat is malicious – a rainstorm might 'exploit' a leaky server room roof, for instance, compromising the availability and possibly integrity of your information systems. Again, confidentiality is not the only aspect you need to protect.

That brings us to the next point – there are not just three aspects of security to consider (CIA), but also three pillars your defences must cover:

1. People
2. Processes
3. Technology

When investing in cyber security, people often focus solely on what technology to implement, overlooking that any technical measures need to be implemented and maintained by people, who need to follow defined processes.

Besides specialist staff, whether internal or outsourced, there is also the internal threat to consider: any authorised user who has access to your systems can be a risk factor. They are often not maliciously motivated, but could have made a mistake like opening an infected attachment. A 2020 Trustwave report found that 50% of all incidents originated from phishing or other forms of social engineering.[2]

Of course, technology can help mitigate these threats to an extent – for instance, by installing anti-malware software and firewalls. However, these solutions are not perfect, even if they can help prevent many common and low-level attacks. You will need some form of staff training and awareness if your employees are to recognise indicators of a cyber attack, such as phishing attempts, and respond accordingly, in line with the appropriate policies and procedures. This will also address issues like people reusing or writing down passwords, which would defy the point of having a strong password policy.

Detection

Even if you put preventive measures in place, those measures might fail, or they may have been implemented to only reduce the impact and not necessarily to prevent the risk from materialising. It is therefore important to consider measures that make you not just cyber secure, but cyber resilient.

Part of being resilient means that you are prepared in the event that your preventive measures fail, because you have combined them with measures to detect and respond to the incident. In other words, detection works where prevention fails. For example, if you invest in a fireproof safe as a preventive measure, the contents in that safe are not actually protected from fire no matter what. Rather, the safe will be able to withstand a fire for as long as indicated by its fire rating – the higher the rating, the longer the safe's contents will not burn. If you pair the safe with a detective measure such as smoke alarms and a responsive measure like sprinklers (more on response later), you can prevent serious harm from being done, even if you cannot prevent fires from happening altogether.

To generalise the safe scenario, a preventive measure may only need to fend off the attack until the response can arrive. This is an important point to take into account as you conduct your risk assessments and decide how to deal with an unacceptable risk – it is not just a case of what your assets might be susceptible to, but also how long they may need to hold out against that threat until support can arrive and take control of the situation. To know when to jump into action and minimise the response time, detective measures play a key role.

There are typically three types of detection to consider:

1. **Pre-incident detection**
   In a nutshell, a form of prevention – trying to prevent the attack or event from happening in the first place by taking appropriate precautions. Concrete activities might include vulnerability scanning and penetration testing.

2. **Real-time detection**
   Where you are not able to prevent the attack outright, you want to know, in real time, when you are under attack. This might be an alarm going off, a security guard spotting an intruder, an automatically generated notification that someone from an unknown IP address uploaded a file to your web server, and so on.

3. **Post-incident detection**
   Unfortunately, most incidents are discovered after the fact. In many cases, this can be months or even years later – the Trustwave report cited earlier also found that 50% of breached EMEA organisations did not detect the breach themselves, and externally detected breaches worldwide took an average of 86 days to be discovered.[3] However, if an attacker managed to breach your security despite your best efforts, you would still want to know about it, and the sooner, the better, so you can perform damage limitation.

Response

Even very reliable detection will not do much good if there is no response. Having an effective prevention–detection–response system in place also improves your cyber resilience and is a form of defence in depth – even if one measure fails, others will stop the attack from being successful or minimise its impact. For example, take the following sequence:

1. Preventive measure: password protection.
2. Detective measure: access logs show a login from an unexpected geographical area.
3. More preventive measures: a second authentication factor (like a one-time password (OTP) sent to a mobile device) and segregation.
4. Responsive measures: force logout; lock the account; change password; forensics (establish what happened); consider defence improvements; share information with regulators (if it was a reportable incident).

As you can see, being prepared for a successful attack enables you to respond effectively. There are, however, different stages of response:

- **Identification** – largely overlaps with detection.
- **Containment** – buying time to figure out exactly what is happening and significantly limit the total damage done by stopping or delaying the attacker.
- **Eradication** – eliminating the root cause of the incident and preparing to restore your systems.
- **Recovery** – ensuring survival; restoring your systems with minimal data loss.
- **Lessons learned** – reassessing the risks, and deciding whether and how you need to change or improve your defences.

IT Governance Cyber Resilience Framework

Admittedly, there is a lot to take in when it comes to cyber security and resilience. In better news, you do not need to do all the legwork yourself – for a start, there are many frameworks available that can offer you an existing and proven structure to work from, reassuring you that you are heading in the right direction. There is a big range to choose from, although in the UK two are particularly common: Cyber Essentials, which has just 5 basic controls, and ISO 27001, which contains a substantial 114 controls, although you are only expected to implement those relevant for you.

Here at IT Governance, we have developed our own Cyber Resilience Framework (CRF). This framework forms a solid foundation for any cyber security project for several reasons:

- It has a comprehensive selection of processes, reducing the odds of overlooking any areas that require security controls.
- This process selection is also extremely flexible – you only implement the measures that you need based on your compliance and business requirements.
- The CRF offers further flexibility in its four maturity levels. This means that, on top of excluding any processes you do not need, you implement the ones you keep only to the level of sophistication that you need.

The CRF also provides a detailed mapping of its processes against four common sets of compliance requirements. Naturally, every organisation must meet different requirements to different degrees, so it is important that you determine exactly what yours are before mapping them against any framework and putting together a detailed action plan.

No matter the size of your organisation, cyber security is no longer optional – it is an essential component of business success and a critical defence against the risks of the information age. The only thing left is to decide when and where your journey will begin.

Cyber Security as a Service

The fastest and easiest route to ongoing cyber security support.

Get unlimited access to the Cyber Security Advice Service, vulnerability scans, staff training, policies and procedure templates, guidance and expert support – all in one simple and affordable annual subscription service.

Assess | Advise | Scan | Train | Document | Support

Find out more ▶

Useful cyber security and resilience resources

IT Governance offers a unique range of cyber security and cyber resilience products and services, including training courses, books, software and professional consultancy.

Managing Cyber Security Risk Training Course

Get a foundation-level introduction to the key aspects of cyber security with this one-day training course. Gain knowledge of cyber security, the threat landscape, threat intelligence, incident response, and more.

CyberComply

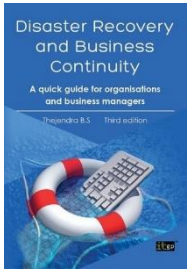
The CyberComply platform makes compliance with cyber security requirements and data privacy laws simple and affordable. Let our software do the heavy lifting, with wizards, databases and prompts to guide you all the way, so you can get started without any expert knowledge.

Cyber Security for Executive Management Instructor-Led Online Training Course

Cover your legal, regulatory and contractual responsibilities in relation to cyber security in this three-hour, instructor-led online course, where you can learn about the biggest threats in cyber security today.

Vulnerability Scanning Service

This fast, fully automated external vulnerability scan of your Internet-facing IT assets enables you to quickly identify vulnerabilities and misconfigurations in your websites, applications and infrastructure.



Disaster Recovery and Business Continuity

A quick guide for organisations and business managers

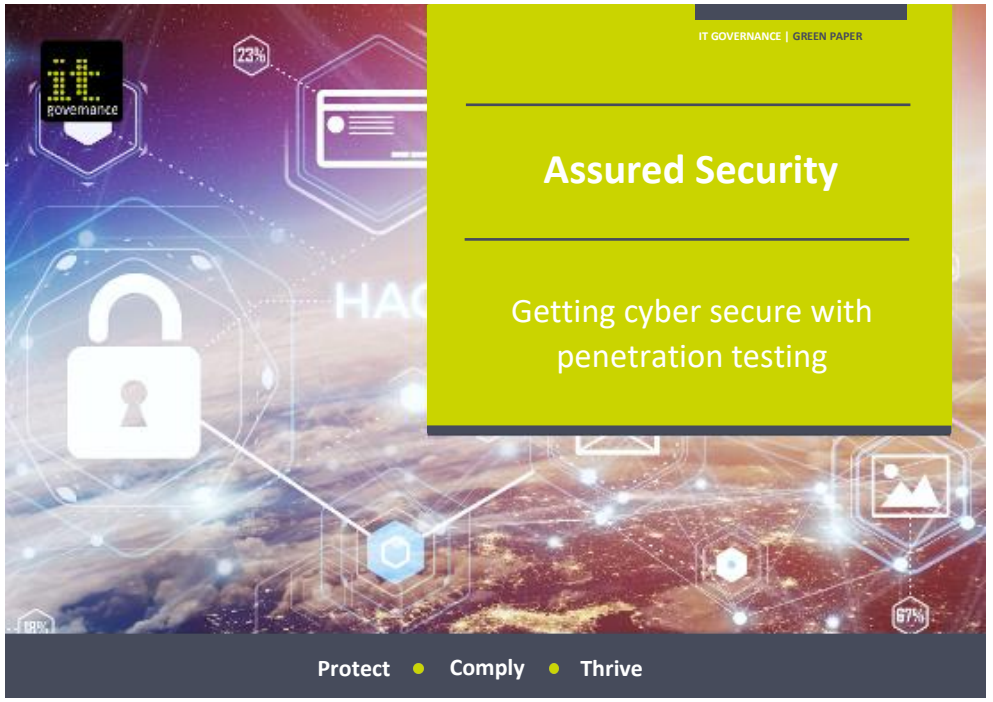
This book explains how to establish a disaster recovery plan, helping you minimise the risks to your business, and highlights the major causes of IT failure and disaster, enabling you to make more effective contingency plans.

Web Application Penetration Test

This CREST-consultant-driven penetration test is designed to identify potential vulnerabilities in your websites and web applications, and provide recommendations for improving your security posture.

Other papers you may be interested in

Cyber Security and ISO 27001 – Reducing your cyber risk



Assured Security – Getting cyber secure with penetration testing

IT Governance solutions

IT Governance is your one-stop shop for cyber security and IT governance, risk management and compliance (GRC) information, books, tools, training and consultancy.

Our products and services are designed to work harmoniously together so you can benefit from them individually or use different elements to build something bigger and better.

Books

We sell sought-after publications covering all areas of corporate and IT governance. Our publishing team also manages a growing collection of titles that provide practical advice for staff taking part in IT governance projects, suitable for all levels of knowledge, responsibility and experience.

Visit www.itgovernance.co.uk/shop/category/itgp-books to view our full catalogue.

Toolkits

Our unique documentation toolkits are designed to help organisations adapt quickly and adopt best practice using customisable template policies, procedures, forms and records.

Visit www.itgovernance.co.uk/documentation-toolkits to view our toolkits.

Training

We offer training courses from staff awareness and foundation courses, through to advanced programmes for IT practitioners and certified lead implementers and auditors.

Our training team organises and runs in-house and public training courses all year round, as well as Live Online and self-paced online training courses, covering a growing number of IT GRC topics.

Visit www.itgovernance.co.uk/training for more information.

Consultancy

We are an acknowledged world leader in our field. Our experienced consultants, with multi-sector and multi-standard knowledge and experience, can help you accelerate your IT GRC projects.

Visit www.itgovernance.co.uk/consulting for more information.

Software

Our industry-leading software tools, developed with your needs and requirements in mind, make information security risk and compliance management straightforward and affordable for all, enabling organisations worldwide to be ISO 27001-compliant.

Visit www.itgovernance.co.uk/shop/category/software for more information.

IT Governance is the one-stop shop for cyber security, cyber risk and privacy management solutions. Contact us if you require consultancy, books, toolkits, training or software.

t: +44 (0)333 800 7000
e: servicecentre@itgovernance.co.uk
w: www.itgovernance.co.uk

A GRC International Group plc subsidiary

Unit 3, Clive Court, Bartholomew's Walk
Cambridgeshire Business Park, Ely
Cambs., CB7 4EA, United Kingdom

IT Governance Ltd

@ITGovernance

/it-governance

@ITGovernanceLtd

Endnotes

[1] UK Department for Digital, Culture, Media & Sport, “Cyber Security Breaches Survey 2020”, March 2020, https://www.gov.uk/government/publications/cyber-security-breaches-survey-2020/cyber-security-breaches-survey-2020.

[2] Trustwave, “2020 Trustwave Global Security Report”, April 2020, https://www.trustwave.com/en-us/resources/library/documents/2020-trustwave-global-security-report/.

[3] Ibid.