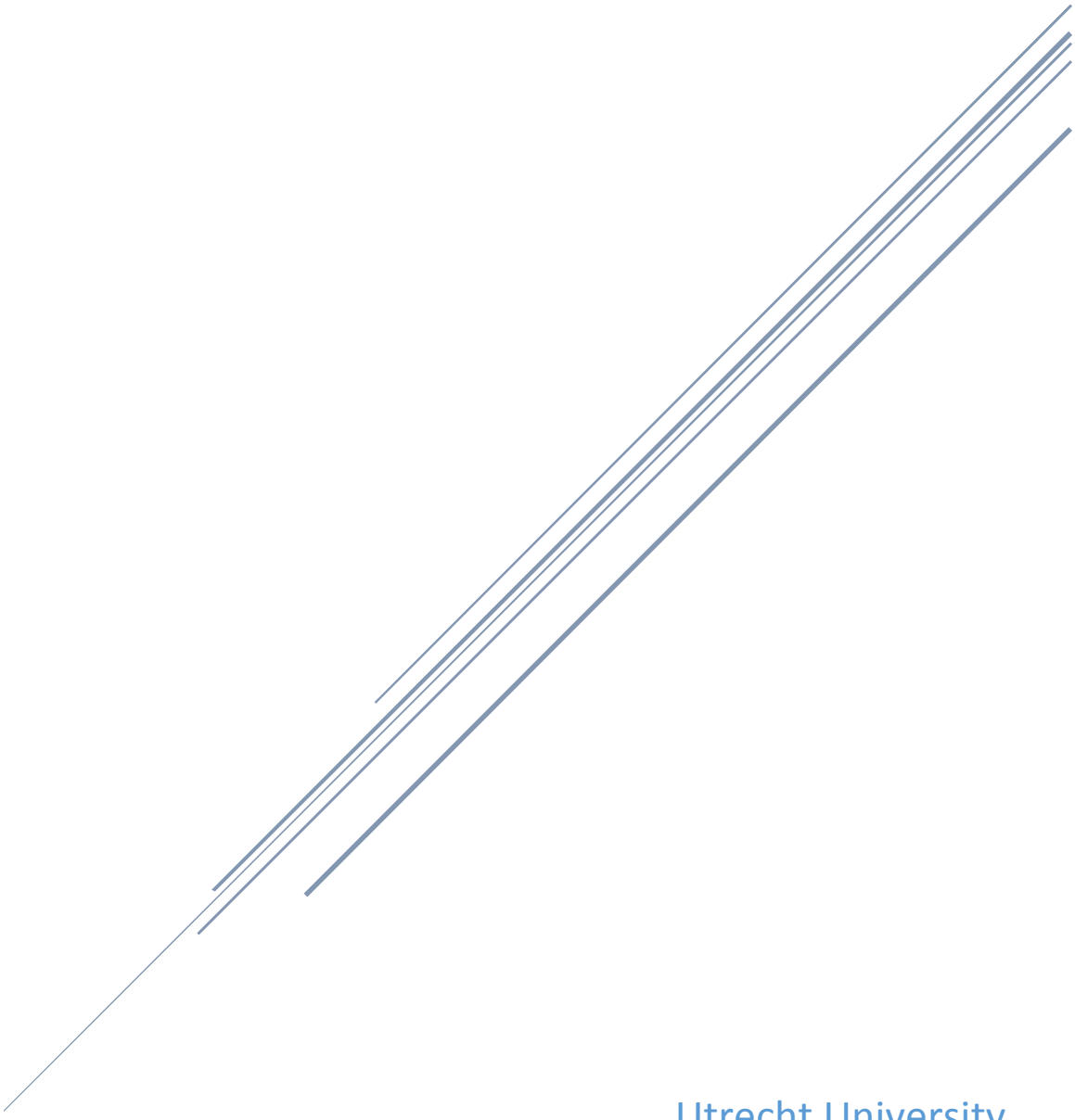
SECURITY OPERATIONS CENTERS

A Business Perspective



Utrecht University
MSc in Business Informatics

Aristeidis Michail

Table of Content

Chapter 1 – Introduction

The information security landscape has shifted tremendously over the past decade. Information security threats have been increasing exponentially both in numbers as well as complexity. To give an indication of the above, Figure 1.1 shows the number of US, federal agency accounted incidents, reported to the United States Computer Emergency Readiness Team for fiscal years 2006 -2014 (U.S. Government Accountability Office, 2015).

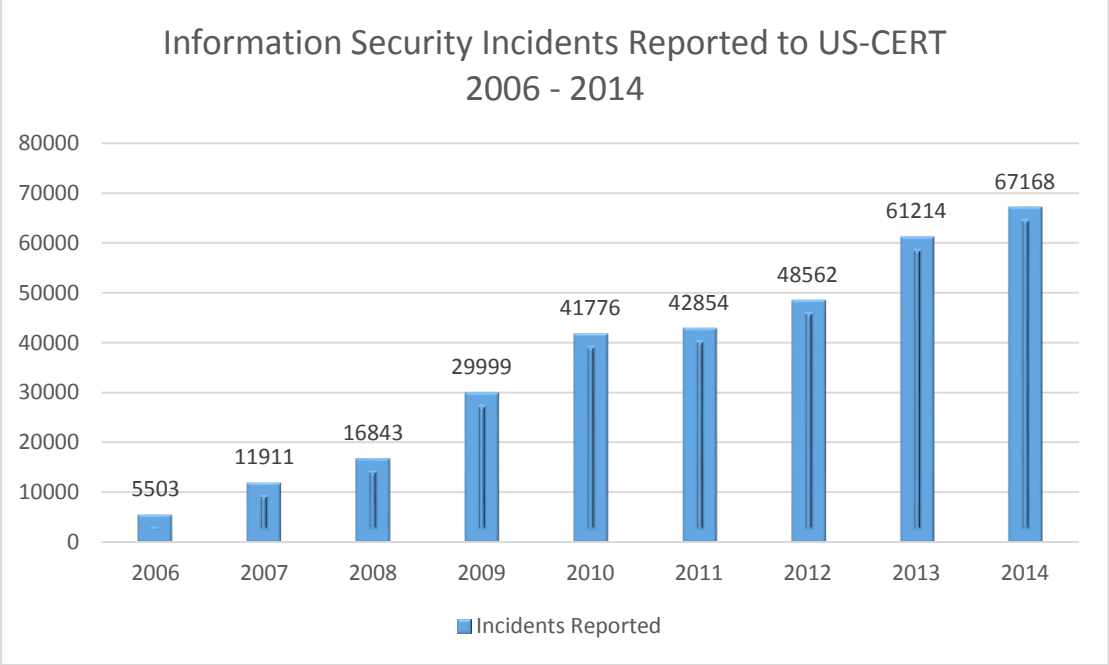


Figure 1.1: US-CERT Reported Incidents for Fiscal Years 2006 to 2012 (U.S. Government Accountability Office, 2015)

Information Security Operations Centers (ISOCs), more commonly referred to as Security Operations Centers (SOCs), are considered a response to the rapidly expanding threat landscape. As early as 1975, SOCs were adopted by the military sector and have undergone fundamental changes in their functionality, capabilities and form since then (Hewlett-Packard, 2013).

The current SOC generation was initially conceptualized by Bidou (2005). In his words, a *"Security Operation(s) Center is a generic term describing part or all of a platform whose purpose is to provide detection and reaction services to security incidents"* (Bidou, 2005, p. 1). A SOC is where the whole of an enterprise's information systems is supervised, assessed, and defended. This is performed by utilizing a combination of people, processes, and technology. Within a SOC, threat related incidents are identified, analyzed, communicated, acted upon, and reported (Li, Hsieh, & Lin, 2013).

Nonetheless, business decision makers are in need of a solid foundation, underpinned both by academic knowledge and real-world based insights, upon which the discussion on whether investing in a SOC is rational and justified can be based. The lack of such a business perspective can be - at least partly - attributed, to the highly technical nature of SOC implementations which cannot be easily linked to C-level executives' goals (Fitzgerald, 2011).

As Walker (2012, p. 17) succinctly puts it *"the lack of a common basis for discussion between security professionals and business decision makers is exacerbated by the generally low level of business*

knowledge/vocabulary in information security. Hence [] the allocation of resources to information security within organizations is likely to be sub-optimal."

The want for such a business outlook of SOCs can also be evidenced in the scientific literature. A preliminary literature search utilizing Google Scholar's database and searching for the possible permutations of the words Security Operations Center in papers' titles produced just twenty five (25) results. Among these papers, only four focused on non-technical SOC aspects. Moreover, no scientific articles could be found showing that SOCs do indeed perform better - information security wise – compared to other possible solutions. For more information on the aforementioned literature search the reader is advised to see Appendix A.

This thesis makes a contribution towards bridging that gap by employing both a theoretical and practical approach. It firstly builds a theoretical background concerning a high level overview of SOCs, their functionalities, the environment in which they operate as well as the business drivers behind their possible implementation. This is achieved through the study of both SOC specific as well as generic information security literature.

Secondly, it employs statistical methods to test whether well-established SOCs do indeed provide superior cyber-security to organizations. Therefore, four principal issues are addressed always from the business executive's macroscopic point of view:

Issue No 1: A lack of clarity exists concerning what a Security Operations Center is and the functions it performs.

Issue No 2: There is a deficiency of a structured high level description concerning the dynamics driving the contemporary information security environment, organizations' adversaries present in it, the technical methods they employ, and the financial impact of their actions.

Issue No 3: There is an absence of a concise summary of the benefits derived from enhanced information security.

Issue No 4: There are no statistical data confirming a Security Operations Center's improved performance concerning information security.

The rationale behind the selection of these issues to form a SOC business perspective is underlined by the theory of Technological Frames of Reference (TFR) as introduced by Orlikowsky and Gash (1994) and extended by Davidson (2002, 2006) as well as Hoppmann, Diaz Anadon and Narayanamurti (2014). By using the TFR theory as a foundation, the building blocks that should comprise a SOC business perspective are defined.

Information Security Definitions

Information security is a relatively young and fast changing field (Nkhoma et al., 2007). Therefore complete standardization of the terms that are used within the field has not occurred yet. In order to enhance readability a list of definitions for the most important terms used in this thesis is provided below (ISO/IEC, 2012).

- Asset: Anything that has value to the organization.
- Attack: An attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset.
- Information Security: The preservation of confidentiality, integrity, and availability of information.
- Information Security Event: An identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant
- Information Security Incident: Single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.
- Threat: A potential cause of an unwanted incident, which may result in harm to a system or organization.
- Data Breach: A compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to protected data, transmitted, stored or otherwise processed.

SOC NAMING CONVENTIONS

The reader should be aware that the term Security Operations Center originates primarily from the information security industry and is not unequivocal. There are other terms that are used to describe organizational formations with functions, capabilities and goals identical to those of a SOC such as Computer Emergency Response Team (Kruidhof, 2014) and Computer Security Incident Response Team (Horne, 2014). In fact, Zimmerman (2014), provides a whole array of synonyms such as Computer Incident Response Team (CIRT), Computer Incident Response Center/Capability (CIRC) and Cybersecurity Operations Center (CSOC).

Additionally, it must be noted that the term security operations sometimes refers to the protection of physical assets and that's why the term cyber is added beforehand for differentiation purposes. This type of security operations is to be considered irrelevant in the context of this thesis. Moreover, in the same context, the term Security Operations Center (SOC) is used to describe all of the aforementioned terms.

The main posit of the TFR theory is that different groups within organizations have different perspectives on the importance and utility derived from technological artefacts. Those incongruences have negative consequences to the effectiveness of IT projects ranging from reduced implementation effectiveness (Barrett, 1999; Olesen, 2014) to completely failing IT projects (Sanford & Bhattacherjee, 2008).

TFR theory examines the perceptions of different groups concerning IT systems through the utilization of three independent qualitative constructs. Those are namely the 'Nature of Technology', 'Technical Strategy', and 'Technology in Use' domains. To draw an analogy they respectively correspond to the 'what', 'why', and 'how' questions concerning the implementation of IT systems.

The TFR theory postulates that initially defining and subsequently aligning those cognitive domains among different member groups leads to improved organizational efficiency through reduced member incongruity. It is important to note that the above means that it's not the use of technology that leads to increased performance. This is achieved by the alignment of perceptions of different organizational groups across the three aforementioned domains. TFR theory is schematically depicted in Figure 1.2 (Larsen, Allen, & Eargle, 2015).

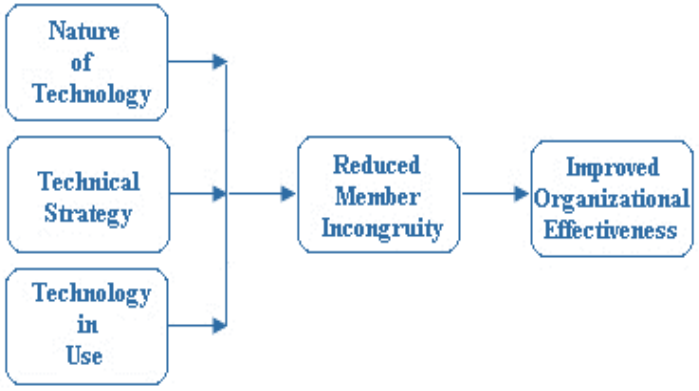


Figure 1.2: Technological Frames of Reference Theory Schematic (Larsen et al., 2015)

The first concept drawn from the TFR theory is the 'Nature of Technology' domain. This domain, incorporates the cognitive frames that relate to an overview of the technological system in question and *"refers to people's images of the technology and their understanding of its capabilities and functionality"* (Orlikowski & Gash, 1994, p. 183). It is therefore directly connected to the first issue mentioned above and forms the first part of our business perspective.

Additionally, when it comes to organizations, prevention of security failures focuses on what is economically optimal (Anderson, 2001). It has also been shown, that one of the critical inputs towards quantifying an ICT security investment is the identification of threats. By having this identification as an input, a proper risk assessment can be conducted (Bojanc & Jerman-Blažič, 2008a).

Subsequently, a second part of a SOC business perspective must be a non-technical summary of the current information security landscape, the security threats it encompasses as well as their implications. The fact that technological frames have been shown to co-evolve with the organizational environment in which they are conceived (Hoppmann et al., 2014) further backs this selection.

Most IT investments are difficult to be justified through traditional financial analysis techniques since the various types of benefits derived from them are difficult to quantify (Ward & Peppard, 2007). The same holds for SOCs with the added problem that information security is considered a risk mitigating function and not a direct contributor to the increase of profit. Adding to that, lack of management support and involvement due to a poor business case has been cited as one of the major causes for failure of technology projects (Whittaker, 1999).

All of these are directly aligned both to the third issue mentioned beforehand as well as to the TFR concept of 'Technical Strategy' which generally refers to drivers behind the adoption of information technologies. This technological frame forms the last part of the business perspective in question.

Figure 1.3 illustrates the chosen method of formation of the SOC's business perspective's theoretical framework. Should the reader compare Figure 1.2 and Figure 1.3 the relation between the SOC business perspective in formation and the TFR model becomes obvious. However, she might also logically question the absence of the 'Technology in Use' domain. This domain of the TFR model refers to *"frames related to incorporating IT into work practices"* (Davidson, 2006, p. 26). The purpose as well as the intended readership of this thesis however are quite divergent from this domain's standpoint.

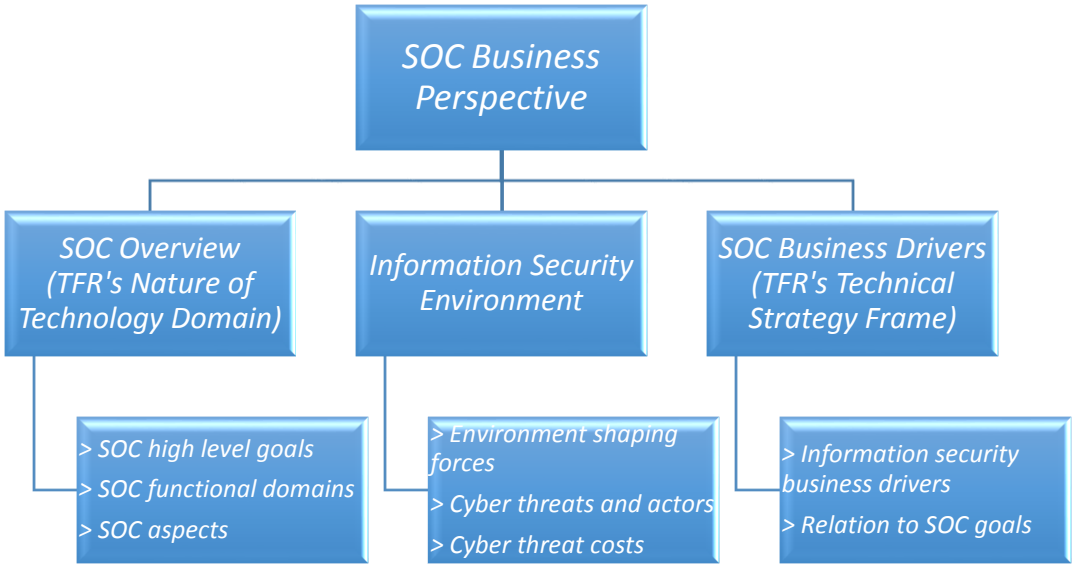


Figure 1.3: SOC Business Perspective Composition

The purpose of building a SOC business centric perspective is to form a high level description of the concepts that should be used while examining and communicating the possibility of a SOC implementation. Moreover, as stated before, this endeavor has been conducted with the business decision maker in mind.

Therefore, the frame domain of day to day operations can be considered as not interesting or relevant enough for her.

Research Questions Definition

This thesis' overarching research question is directly related to all of the above and has to do with examining the structural components of a real-world SOC business case. It has been defined as follows.

Overarching Research Question: *Given the business executive's standpoint, is there an alignment between Security Operation Centers' goals and capabilities with the contemporary information security environment's requirements that can lead to business benefits being harvested by organizations and if so, is that the case in practice?*

In order to approach our main research question three research questions have been defined. The first one, further subdivided into three sub-question, follows closely the rationale of the SOC business perspective described beforehand and examines its three structural components.

Research Question 1: *How can Security Operations Centers be viewed from a business decision maker's perspective?*

Taking our cues from the TFR theory and following the approach described beforehand, this research question can be sub-divided into three separate research sub-questions.

Research sub-question 1.1: *What is a high level description of a SOC concerning its goals, functions, and operating aspects?*

Research sub-question 1.2: *What is the state of the art when it comes to information security? What are the field's shaping forces and the main threats and threat actors towards organizations?*

Research sub-question 1.3: *What are the business drivers underlying a SOC implementation and the enhanced information security performance it could provide?*

Each of these research sub-questions has been tackled by extensively reviewing scientific as well as industry literature and connecting the findings to SOC capabilities and functionality. The findings derived from this analysis advocated for SOCs being indeed fit for the contemporary information security environment thus enabling organizations to realize various significant business benefits. It was therefore deemed necessary to examine whether this fitness is realized through superior information security performance in real world situations. Therefore this thesis second research question has been defined as follows.

Research Question 2: *Does the existence of a well-established Security Operations Center lead to better organizational performance concerning information security when it comes to the hacking, card fraud, and insider data breach types?*

To tackle the aforementioned research question, a publicly available database of data breaches that have occurred over the last ten years in the United States has been used. By utilizing a matched pairs sampling method, the breaches that have occurred in organizations with an embedded SOC are compared in terms of size to those that occurred in organizations without one.

The data breach types mentioned in our second research question are the ones SOCs are directly fit to protect organizations from. They are not however, the only ones occurring in practice. It was therefore found valuable to examine, per industry, whether there is a significant difference in their impact compared to other types of data breaches. This analysis is not only academically interesting but can also be used in order to determine whether certain industries can benefit by prioritizing SOC investments. All of the above lead to our third research question.

Research Question 3: *Which industries among the financial, insurance, medical, nonprofit, government, and retail ones are significantly differently impacted by data breach types relating to SOCs compared to data breaches unrelated to SOCs?*

Thesis Structure

This thesis is divided into two parts in accordance to the research questions defined beforehand. The first part is concerned with building the proposed SOC business perspective and serves as an answer to our first research question. It consists of chapters 2 to 4. Each of these chapters is related to one of the sub-questions defined above respectively.

Chapter 2 is concerned with defining a SOC. It describes its goals and the problems it aims to solve, its functional areas as well as the different aspects that define it. To do so a mixture of scientific and industry literature has been analyzed with the balance leaning towards the latter. This is a direct outcome of the scarcity of purely academic literature concerned with SOCs from a high level or business viewpoint.

Chapter 3 deals with the current information security environment. It describes its defining forces, the types of different actors involved as well as the types of threats that it encompasses. Moreover, it provides an overview of the costs inflicted to organizations due to information security mishaps. It therefore provides a concise description of the environment in which a SOC will operate.

Lastly, Chapter 4 draws from academic literature to uncover the business drivers behind information security implementations. Given that a SOC's goal can be effectively summarized as superior information security this is an essential component of its business perspective. At the end of the chapter our SOC business perspective is presented.

The second part of this thesis, consisting of chapters 5 and 6, is concerned with framing our business perspective with insights drawn from real-world data. Those chapters describe the statistical methods used in order to answer our second and third research questions respectively.

A Process Delivery Diagram (PDD) is a meta-modelling technique introduced by van de Weerd and Brinkkemper (2008) involving the integration of a meta-process and meta-deliverable model on its left and right sides respectively. The deliverables are straightly derived from the processes connected to them. Moreover they can be used as input for processes occurring after their creation. Figure 1.4 - located on the following page for readability purposes - illustrates this thesis' structure and research approach using a PDD.

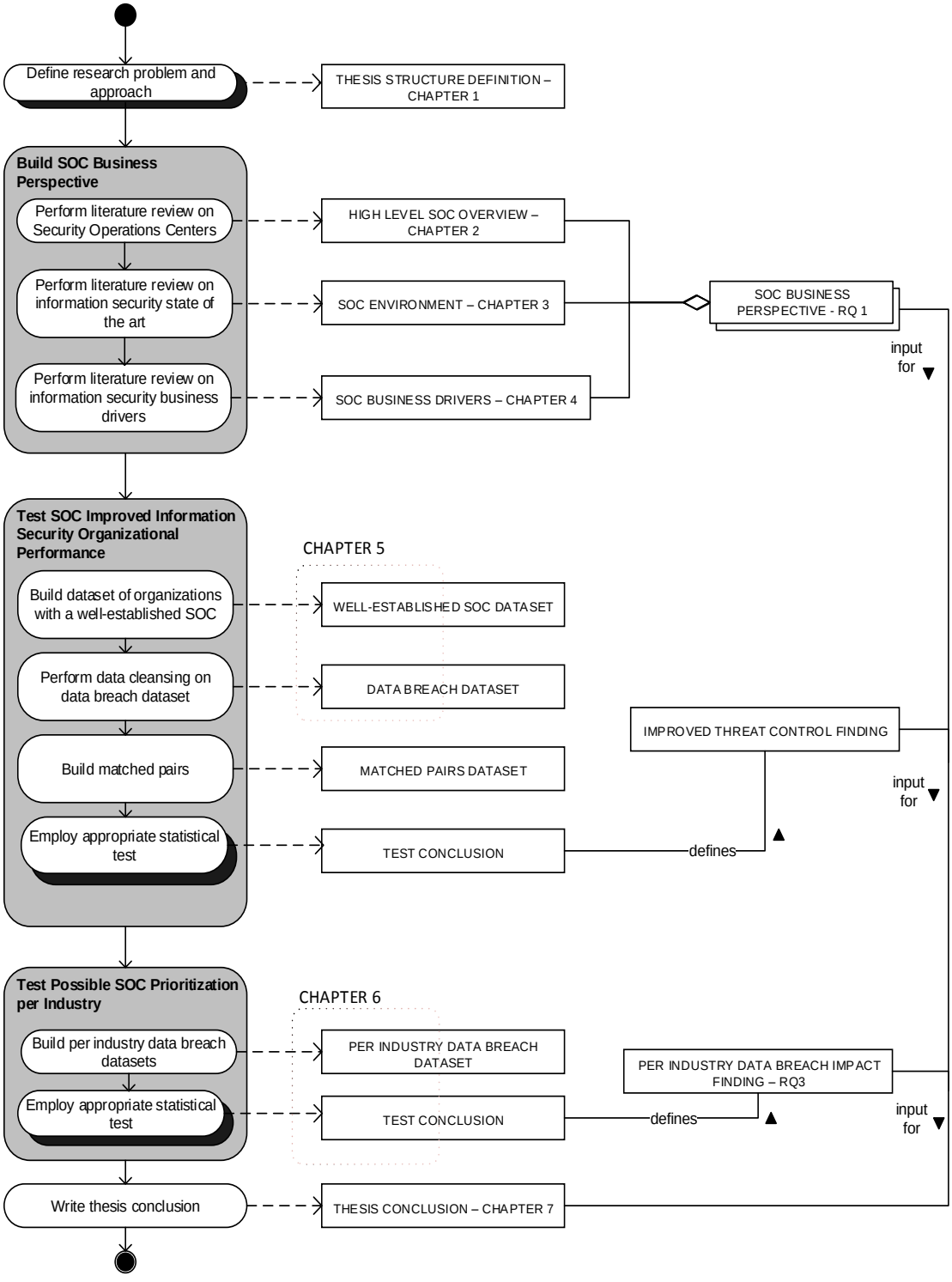


Figure 1.4: Thesis Structure PDD

Chapter 2 - Overview of Security Operations Centers

In order to build the first pillar of our proposed SOC business perspective and answer the respective research sub-question this chapter will give an overview of Security Operations Centers.

Before diving into details a point that needs to be drawn is that a SOC is not a predefined entity. It is not a particular technological system that is deployed in order to defend against specific security threats. It is rather an organizational structure - underpinned by technological solutions - that attempts to manage and enhance the overall security posture of organizations. As it will become evident in this chapter, this is done by utilizing a combination of people, processes, and technology. Each of those elements - as well as their smooth cooperation - is critical to a successful SOC implementation.

The chapter's logic is this: It initially illustrates the information security gaps that the existence of a SOC intends to fill. Continuing, typical high levels goals of a SOC implementation are introduced. Afterwards, the functional domains that characterize a SOC, through which those high levels goals are attained, are illustrated. Lastly, the three aspects that are combined (technology, people, and processes) to form a SOC are presented.

Current Security Solutions' Limitations

For quite a while enterprises have been deploying point solutions such as firewalls, antivirus software and intrusion detection or prevention systems (IDSs/IPSs) in order to protect their assets. As their naming implies point solutions are information security protective measures designed to monitor and protect only a specific segment of the IT infrastructure. To give an example firewalls are only concerned with filtering network traffic while antivirus software is occupied with eliminating unwanted and malicious applications from systems. Those two solutions, present in most contemporary systems, operate often unaware of each other's existence.

This castle approach as it is sometimes termed, proved to be problematic due point solutions' limited scope of protection and cooperation. One of the early emblematic cases of diminishing protection capabilities was the 2003 computer worm Slammer that managed to infect about 75000 systems in less than 10 minutes (Moore, Paxson, & Savage, 2003). Despite the impressive numbers what is really important and indicative of this case, is the fact that its remediation required the combined efforts of *" firewalling, scan-signature detection at port 1434, and system patching"* (Forte, 2003). It therefore required an understanding of different domains of the IT stack and coordinated action between the solutions protecting them.

Currently the attack methods Slammer used are considered outdated. Modern dangers such as Advanced Persistent Threats (APTs) simultaneously utilize a varied range of attack vectors and patterns thus making their detection by point solutions an almost unachievable task (Thomson, 2011).

Adding to that, point solutions produce a massive amount of logs thus resulting to a deluge of data. Those log files are closely related to both intrusion detection and network forensics (Forte, 2004). To give a more quantifiable perspective *"average quantities in incident response tasks are on the order of fifteen target objects [] and two terabytes of data"* (Forte, 2008, p. 14).

IT security personnel find it very hard to go through, understand and act upon this data. This condition can be worsened by the fact that security solutions might be geographically dispersed and/or managed by different teams. Teams which in their own turn possibly use different tools (Hewlett-Packard, 2011a). This results into impacted costs without necessarily increasing the security level of an organization since effective security strategies turn out to be infeasible in large scale networks (Li et al., 2013).

In the next section the requirements a SOC must fulfill in order to overcome those challenges will be described.

High Level SOC Goals

The goals a SOC must effectively fulfill, derive as a natural outcome of the limitations previously discussed. In order to achieve complete alignment with the organization at hand, both SOC architectures and goals might slightly differ. Nonetheless, both scientific and industry literatures seem to coalesce across the vectors introduced below (Amoroso, 2011; IBM Global Technology Services, 2013; Kelley & Moritz, 2006; NASA SOC, 2010).

Situational awareness deliverance

Organizations need to be at all times informed about what is happening across the whole of their IT infrastructure. The only way that this can be delivered is by the aggregation, association, and contextualization of the sum of data streams that multiple devices produce. A SOC must be able to consolidate those streams so that a holistic view of the security posture of an organization is constantly available.

Risk and downtime reduction

The global economy dictates that organizations must be able to perform business around the clock. Switching off an infected system such as a web application server is no longer an option. A SOC must be able to leverage its advanced protecting capabilities in order to proactively defend the enterprise (Hewlett-Packard, 2013). This means alerting the right people at the right time and closing security holes in a timely manner. Adding to that, risk reduction is the founding pillar of information security investment justification (Derrick Huang, Hu, & Behara, 2008; Gordon & Loeb, 2002).

Threat control and prevention

The threat landscape has been moving at a frantic pace in the past decade during which vulnerabilities and threats have significantly increased. This suggests that in order to achieve threat prevention, a SOC must not only constantly refine its imposed defenses but also leverage external partnerships in order to remain up to date.

Nonetheless, an absolutely secure system is not feasible. When a threat achieves network penetration it must be identified and isolated early on in the 'kill-chain' in order to minimize its impact (Hutchins, Cloppert, & Amin, 2011).

Diminishing of administrative overhead

As Kelley and Moritz (2012, p. 29) concisely put it, one of the main goals of a SOC is *"to empower a few administrators with the best information to enable fast, automated responses"*. This is done by collecting data from automatically monitored point solutions. Data that are subsequently analyzed and correlated thus providing a condensed depiction of the near real-time security posture of an organization. This depiction can be visualized in a central screen, greatly augmenting SOC operators' problem solving abilities during the all-important triage phase (Stolze, Pawlitzek, & Wespi, 2003), thusly minimizing human overhead.

Forensics

Suppose that a threat managed to penetrate the defences but was ultimately remediated. In order to ensure that this or similar used attack patterns won't be able to be utilized against the enterpise again there is the need to identify its root cause. By having structured log data provided by the SOC, security analysts are able to perform this kind of investigation (Casey, 2008).

Audit and compliance support

Audit and compliance support has been an important goal for SOC implementations in the past decade. During this period a variety of regulatory standards have emerged like SOX, HIPAA, PCI DSS, and the EU Data Protection Act. Irrespective of their intended impact a common denominator of those standards is the retaining of various security logs at increasingly granular levels and for extended time period (Madani, Rezayi, & Gharaee, 2011). To give a time span perspective Table 2.1 shows the log storage duration time of some common frameworks.

Normative Standard	Years of log retention
HIPAA	6 or 7
SOX	7
PCI DSS	1

Table 2.1: Years of Log Retention According to Normative Standards

It is obvious that this requirement results in a sizeable amount of security log data that need to be available at any given point. Those data are generated in distinct parts of the IT infrastructure. A SOC must therefore not only be able to collect and store those logs but also retrieve them as easily as possible in order to minimize the effort while preparing for a possible audit.

SOC Functional Domains

In order to fulfill the aforementioned goals a SOC must be able to perform certain actions. This section, groups those actions under more general SOC functionalities termed functional domains. What is noteworthy, is the fact that the mapping of higher level SOC goals to functional domains is not a one to one relationship. The case here, is that a single functional domain might support different higher level goals. This becomes evident in Table 2.2, located at the end of this section, where the complete mapping of goals to functional domains is summarized. The functional domains that are presented below are the least needed in order for a SOC to be able to effectively accomplish all of the aforementioned goals.

Log Collection

A SOC centrally collects all logs produced that concern any security, system or transactional activities. Since a SOC acts as an aggregator of data produced by point solutions it is important to collect information from a multitude of systems independently of the sources' characteristics such as vendor or used protocol. The Intrusion Detection Message Exchange Format has been proposed as solution to the interoperability issue (Lin, Wong, & Wu, 2005). Log collection relates to the situational awareness deliverance, forensics, and audit and compliance support SOC requirements.

Log Retention and Archival

The logs collected by the SOC must be centrally stored and easily recovered. There are multiple motivations behind this. After an attack has occurred the logs will be used in order to perform forensics and determine the vulnerability that was taken advantage of. Moreover, logs need to be kept for compliance purposes. Lastly, they can be used to provide historical data so that patterns of normal systems' behavior (e.g. network traffic) can be defined. Any deviation from those patterns might signal an ongoing attack on the enterprise systems. Therefore, log retention and archival relates to risk and downtime reduction, threat control and prevention, diminishing of administrative overhead, and audit and compliance support.

Log Analysis

Logs usually contain exclusively raw data. SOC's technology should have the ability to extract useful information such as relevant metrics, out of this data. Log analysis relates to situational awareness deliverance, diminishing of administrative overhead, and threat control.

Monitoring of Security Environments for Security Events

The ITIL glossary's definition of monitoring is "*Repeated observation of a configuration item, IT service or process to detect events and to ensure that the current status is known"* (Hanna & Rance, 2011, p. 49). In a SOC context this means that the information provided by log analysis is presented to analysts in a comprehensible manner. Security analysts are thus enabled to determine the current security posture of the organization. Monitoring relates to diminishing of administrative overhead, situational awareness deliverance, downtime reduction, and threat control.

Event Correlation

A SOC should have the ability to automatically correlate and contextualize events from different event sources. This automatic correlation is based upon a set of predefined correlation rules. The intelligence underlining those rules can be the difference between timely attack detection and an unobserved security incident. Moreover, the rate of reported incidents that do not represent a threat (false positives is the accepted industry term) can be significantly diminished by proper correlation rules. Event correlation relates to situational awareness deliverance, downtime reduction, threat control, and reduction of administrative overhead.

Incident Management

Incident management refers to the processes and procedures that direct the escalation and reaction towards a reported security incident. Since the number of reported incidents in the day to day SOC operation is quite large, incident management is needed in order for the SOC's resources to be utilized in an efficient manner. This efficiency is achieved through prioritization of incidents according to predefined rules and objectives. Incident management relates to risk and downtime reduction as well as threat control.

Threat Identification

Threat identification refers to a SOC's ability to correctly identify threats and vulnerabilities both in real time as well as a pro-active measure deriving from research. While such a functional domain is fairly obvious the constantly evolving security threat landscapes dictates that a successful SOC will be able to keep up to date by leveraging external partnerships and having training programs in place among others. Threat identification is related to threat control and prevention.

Threat Reaction

Naturally, a SOC needs to be able to able to react to threats both reactively as well as proactively. Reactively suggests immediate remediating action as soon as an identified threat is spotted in the network. Proactively means finding security gaps in the infrastructure or processes and remediating the situation before an attack can exploit it. Threat reaction is related to threat control and prevention.

Reporting

A SOC must be capable of offering its clients detailed security reports. The reports should be flexible enough so as to cover multiple requests ranging from real-time management to audit requirements. Due to its nature, reporting is related to all of the SOC high level requirements.

Depending on the scope of the SOC various other secondary functional domains can be defined such as malware analysis, vulnerability scanning and analysis, device management, penetration testing, physical security controls integration, and industry verticals monitoring (Jacobs, Arnab, & Irwin, 2013).

Table 2.2 summarizes the mapping between a SOC's higher level requirements and its functional areas. It is worthwhile to note that many requirements necessitate the cooperation of multiple functional areas. This gives a first glimpse of the complexity that is involved in a SOC.

SOC High Level Goals	SOC Functional Areas
Situational awareness deliverance	Log Collection, Log Analysis, Monitoring of Security Environments, Event Correlation, Reporting
Risk and/or downtime reduction	Log Retention and Archival, Monitoring of Security Environments, Event Correlation, Incident Management, Reporting
Threat control and/or prevention	Log Retention and Archival, Log Analysis, Monitoring of Security Environments, Event Correlation, Incident Management, Threat Identification, Threat Reaction, Reporting
Diminishing of administrative overhead	Log Retention and Archival, Log Analysis, Monitoring of Security Environments, Event Correlation, Reporting
Forensics	Log Collection, Reporting
Audit and compliance support	Log Collection, Log Retention and Archival, Reporting

Table 2.2: SOC High Level Goals and Functional Areas Mapping

In the following section the combination of technology people and processes that a SOC uses to achieve this functionality is going to be illustrated.

Bringing it All Together: Technology, People, and Processes

The technology, people, and process model has been used in information science literature for a variety of topics spanning from knowledge (Pee & Kankanhalli, 2009) and customer relationship management (Chen & Popovich, 2003) to process improvement (Prodan, Prodan, & Purcarea, 2015). It has also been adopted to effectively describe the triad of aspects cooperating and effectively comprising a SOC (Andress, 2004; Hewlett-Packard, 2009; IBM Global Technology Services, 2013) those of course being people, processes, and technology.

A perhaps oversimplified description of the interplay between those aspects would be that technology gathers the sheer volume of data produced by point solutions and consolidates it into information that people can act upon. At the same time processes ensure uninterrupted SOC operations while also being the glue that holds the other two aspects together.

What will become apparent (especially after the technology aspect subsection) is the fact that a SOC constitutes, more than anything, an organizational structure. As such it needs to be well managed since even two of the aspects alone cannot deliver the higher level goals introduced previously.

The Technology Aspect

A SOC utilizes a plethora of technical solutions which can vary a lot depending on the SOC's scope and mission. However, the technologies presented below are used in all of modern SOCs and are considered the backbone of the technological aspect.

Security Information and Event Management system (SIEM)

A SIEM system is the technology that underpins every action occurring at a SOC. This system acts as the aggregator, distiller, and correlation engine of the data acquired by the point security solutions. Any SIEM system can be roughly divided to a Security Information Management (SIM) and a Security Event Management (SEM) system (Nicolett & Kavanagh, 2011). The former is primarily concerned with log management and compliance reporting whereas the latter with security real-time monitoring, incident management, and threat remediation.

Capabilities of a SIEM system include:

- Data aggregation and retention
- Correlation
- Alerting
- Dashboards
- Compliance
- Forensic Analysis

It can be discerned that the capabilities of a SIEM closely match the high level requirements of a SOC. The two are so closely linked that scientific literature exists that while using the term Security Operations Center, it in fact describes SIEM system architecture (Karim Ganame, Bourgeois, Bidou, & Spies, 2008). Lastly, the reader should note that the technical solutions that follow should be directly connected to the SIEM system.

Database Activity Monitoring (DAM)

DAM oversees the usage of selected databases. It detects unusual activities of privileged users or administrators so as to ensure that compliance objectives are met and no actions that could hurt data integrity or availability are performed. If such behaviors are detected the database automatically issues an appropriate response (Kamra, Bertino, & Nehme, 2008).

Intrusion Detection Systems (IDSs)

IDSs are devices or applications that intend to detect malicious behavior that is targeted against a network and its resources. They do so in two ways. The first is to search for predefined patterns of malicious behavior called signatures. This approach is labeled as misuse-based. The second is to detect deviation from an expected behavior (anomaly-based). Both approaches have their strengths and weaknesses which have been extensively reviewed by various researchers (García-Teodoro, Díaz-Verdejo, Maciá-Fernández, & Vázquez, 2009; Patel, Qassim, & Wills, 2010; Shameli-Sendi, Cheriet, & Hamou-Lhadj, 2014). Lastly another categorization of IDSs comes from the source of events they analyze. Thus host-based, application-based and network-based IDSs exist.

Intrusion Prevention Systems (IPSs)

IPSs are very similar to IDSs in the sense that they both monitor a specific source of events. The main difference among them is that the former are also able to actively block detected intrusions (Scarfone & Mell, 2007).

Firewalls

Firewalls control network traffic by logically separating interconnected computers into trusted and distrusted zones. This separation is performed on the basis of an applied rule set. The Web Application Firewall (WAF) is considered especially important since besides ensuring secure internet communication it also produces logs that can be used for forensics and reporting (Luthra, Sharma, Gahlot, & Gahlot, 2013).

The People Aspect

When it comes to information security, if there is one thing that needs to be understood, it is that the most important actions are always performed by people. As mentioned before one of the goals of a SOC is to empower security personnel with timely, accurate, and contextualized information so that it can use them to mount effective responses. Responses that the technology underpinning a SOC cannot perform on its own. A depiction of the alert information flow in a SOC is illustrated in Figure 2.1 (Forrester Research Inc., 2013).

Depending on the SOC's size, mission and implementation a number of tiers of analyst exist. Each tier must have a set of unequivocal responsibilities while the escalation path among the tiers must adhere to a predefined procedure.

Staffing a SOC is not an easy process due to the multitude of both technical and soft skills that personnel should be in possession of. Adding to that a study performed by the International Information Systems Security Certification Consortium ((ISC)^2) revealed a shortage of capable security professionals on the international market (Suby, 2013). Table 2.3 provides a non-exhaustive overview of the typical skill set of a SOC analyst.

Hard Skills	Soft Skills
Operating System Proficiency	Communication Skills
IDS/IPS	Proactive Mentality
Multiple Hardware Platforms	Continuous Learning Abilities
Database Analysis and Operations	Customer Relationship Skills
Programming Languages	Analytical Mindset and Problem Solving Abilities
Network Protocols	Ability to Perform Under Stress
Applications	Ethics
Attack Patterns and Threat Awareness	Abstract Thinking

Table 2.3: Typical SOC Analyst Skill Set

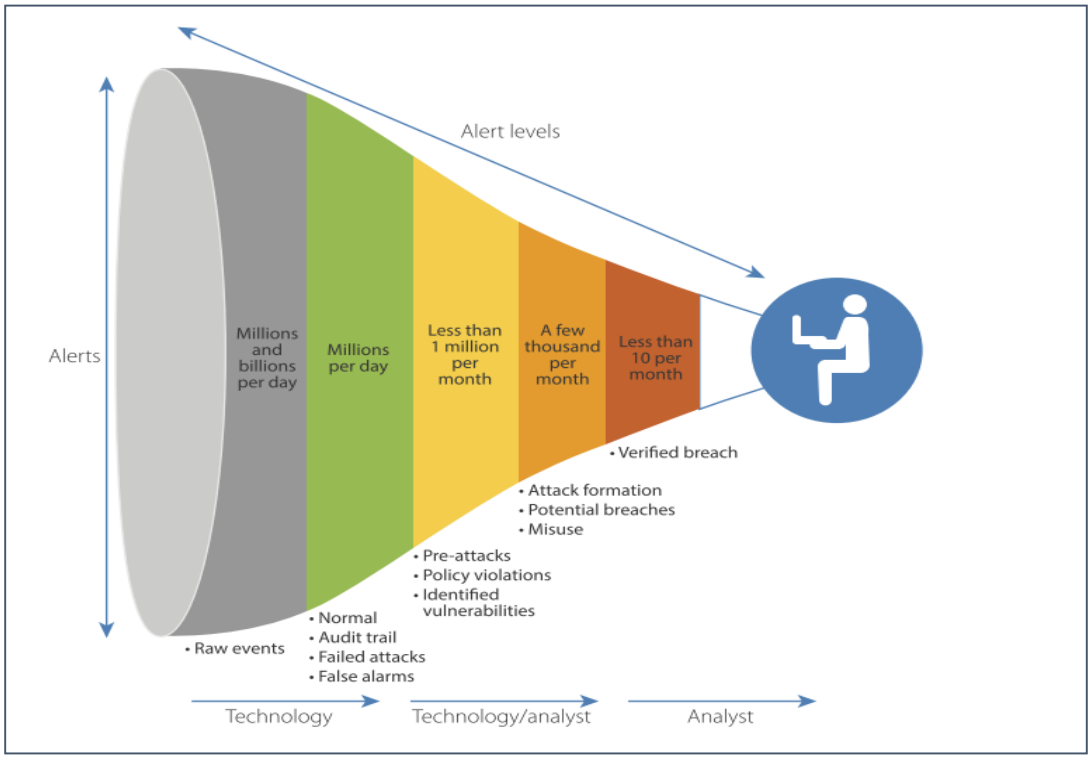


Figure 2.1: Alert Information Funnel (Forrester Research Inc., 2013)

Given the aforementioned shortage, an important issue concerning a SOC's people aspect is the fact that security analysts have a limited 'shelf life'. This is caused by the fact that (especially in SOCs that operate in a 24x7 timeframe) analysts work long hour, tiresome shifts. As a result a typical term of a SOC analyst is between one and three years. Employee retention is made even more important by the fact that analysts

use tacit knowledge to perform their duties, pertaining to the specifics of the organization's IT infrastructure (Goodall, Lutters, & Komlodi, 2009).

Besides security analysts other typical roles that can be found within a SOC are (Hewlett-Packard, 2011a; McAfee, 2012):

- Security Specialists
- Security Engineers
- Forensics Investigators
- Threat Investigators
- SOC Managers

Processes Aspect

Processes can be thought of as the interfaces which the other functional parts of the SOC utilize in order to cooperate. Adding to that, they ensure the seamless and effective operation of a SOC. Especially important ones are the processes that act as a gap filler between the people and technology aspects (Haight, 2014). SOC processes can be divided into four categories (Hewlett-Packard, 2011a; IBM Global Technology Services, 2013):

- Business processes
- Technology processes
- Operational processes
- Analytical processes

Business processes define and document the administrative components required to efficiently operate a SOC while guaranteeing that the operations are aligned to organizational goals. Examples of such processes are report preparation, log retention, definition of security policy and assurance of adherence to it.

Technology processes ensure that the IT infrastructure performs at optimal levels at any given time. They also maintain the information and document the actions pertaining to system configuration management, system administration, technology integration etc. Examples of such processes are vulnerability scanning and remediation, firmware and software updating as well as software patching.

Operational process document and define the actions that are performed on a SOC on a day to day basis. Examples of such processes are shift scheduling and turnover as well as employee training.

Lastly, analytical processes determine how security issues are detected and remediated. They also include the actions taken in order to learn about and understand surfacing threats. Examples of such procedures are incident classification, detection and escalation, ticketing and forensics.

Chapter Conclusion

In this chapter a high level overview of a SOC's goals, functional domains, and comprising aspects has been presented. The most important insight deriving from this overview is that a SOC is not a system specifically designed to protect against particular threats by performing predefined actions. This is not in dissonance with the previously mentioned SOC definition proposed by Bidou (2005, p. 1) describing a SOC as *"a generic term describing part or all of a platform whose purpose is to provide detection and reaction services to security incidents".*

In fact we can assume that the use of vague terms such as 'generic' or 'platform' is very well intended because a SOC is an organizational structure, encompassing multiple systems, that increases the protection level of organizations by orchestrating those systems though the coordination of its people, processes, and

technology aspects. We can also see however, that although detection and reaction services remain the core purpose of SOCs their goals could be extended to include audit and compliance support as well as diminishing of administrative overhead.

The aforementioned systems could be very well present in the IT infrastructure of an organization without the existence of a SOC. This fact highlights that orchestration is the key difference. In its own turn, this statement stresses the importance of well thought and unambiguous processes.

What's more, within a SOC, people remain both the decision makers as well as the ultimate action takers. This advocates for the fact that investing in technology just for its own sake will not yield the desired results. It is people with broad technical expertise, possessing tacit knowledge of an organization's specificities that can harvest the SOC's infrastructure's capabilities and enhance the security posture of businesses.

Thusly a high level of complexity is embedded in every SOC implementation. Therefore, like any other multipart organizational structure a SOC needs first and foremost to be well managed in order to perform appropriately.

SOC management should start with clearly defining all of the characteristics of the SOC's relation to the organization it protects. Issues like what are the SOCs exact goals, how they should be prioritized, and through which SOC provided services they are offered should be in accordance with the host organization's needs and be clarified from the start. Moreover, a SOC should be given the power and authority to act upon detected incidents through established processes.

Figure 2.2: A SOC Model

All of the above, will influence the technologies that are going to be used by a SOC, the structure of its inwards and outwards facing processes as well as the skills its people should be in possession of. Thusly, the exact form that a SOC implementation will have. This is depicted in Figure 2.2 presenting a model of our proposed model.

Nonetheless, the aforementioned matters should be resolved while having the current information security environment in mind. We will examine this environment in the following chapter.

Chapter 3 - The Information Security and Cyber Threat Landscape.

A Security Operations Center acts as a guarantor of information security at an enterprise. Nonetheless, before implementing one, organizations should be aware of today's defining forces of the information security landscape as well as of the current and emerging threats towards them. Therefore, this chapter's aim is twofold.

It initially provides an overview of the realities that shape the current information security landscape. This is done so as to establish the setting under which a SOC will operate and underline the importance of some of its functions. Secondly, the current threat landscape is presented so as to establish what damage present-day threats are capable of delivering and the methods they use in order to do so. Lastly, financial data concerning incurred costs are presented too.

Combined, those two landscapes will give a complete picture of why information security should be prioritized in the minds of decision makers as well as the barricades in implementing it. In the context of this thesis, the importance of having such an overview can be summarized in the words of Fitzgerald (2011, p. 247): *"Communicating with the C-suite requires a different language from what is normally used with the end users or technical staff".*

This chapter aims to fill this communication divide by providing a high level overview of the aforementioned landscapes and relating them to a Security Operations Center capabilities. Moreover, when contrasting a SOC's capabilities to information security obstacles as well as to the methods adversaries employ, the SOC's added value towards more stable and lower risk business making becomes evident.

The Information Security Landscape

Information security has for a long time been considered the by-product of conducting business through the use of Information and Communications Technology. The sub-sections below aim to describe the current shaping forces of information security so that an opinionated view on whether the aforementioned view should still be the case can be formed.

Adversaries' Motivation and Freedom of Action

One of the most major shifts in the information security landscape over the past decade has been the change in attackers' motivation. Initially, most security incidents were caused by adversaries with relatively limited means and the intent of proving that they are able to bypass security measures. In other words the main motivational factors of adversaries were pride and reputation (Bowles, 2012). Although this still holds to a certain degree, the major incentives of cyber-crime practitioners have changed.

Attackers are now mainly led by financial profit (Franklin & Perrig, 2007). A whole industry and ecosystem are presently existent based on monetary gains derived from cyber-attacks. To give an indication of the level organization of this industry, black markets exist where criminals with highly specialized roles trade between them (Rob & Martin, 2006).

What's more, it has been shown that the vast majority of cyber-crimes remains unpunished due to the fact that federal authorities are not able to keep up with the pace of technological change (Gogolin, 2010). Adding to that, authorities have established cross-border cooperation mechanisms only for serious crimes unrelated to cyber offences (e.g. drug trafficking). Given the transnational nature of cyber-crime the result is the same as when offenders started using cars and authorities needed a *"generation to catch up"* (Moore, Clayton, & Anderson, 2009, p. 6).

In his canonical work, Nobel prize winner Gary Becker concluded that under such circumstances of non-control, it is only rational for offenders to actually perpetrate crimes since the rewards are much higher than the possible penalties (Becker, 1968). By reversing his position, it can be surmised, that a working SOC can protect the organization by its mere existence. In other words a rational and financially motivated attacker will pick targets where he can easily achieve the maximum return on investment. Therefore, a well-functioning SOC will act as a security deterrent since the cost of launching an attack against it would be higher. To put it simply, such an adversary would pick softer but equally lucrative targets.

Software Vulnerabilities Issues

Given that without them the vast majority of attacks would be nonexistent, vulnerabilities constitute one of the most fundamental concepts in information security. According to the U.S. National Institute of Standards and Technology (2012, p. 18) *"a vulnerability is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source"*. The central role of vulnerabilities in information security is depicted in Figure 3.1 (ISO, 2009).

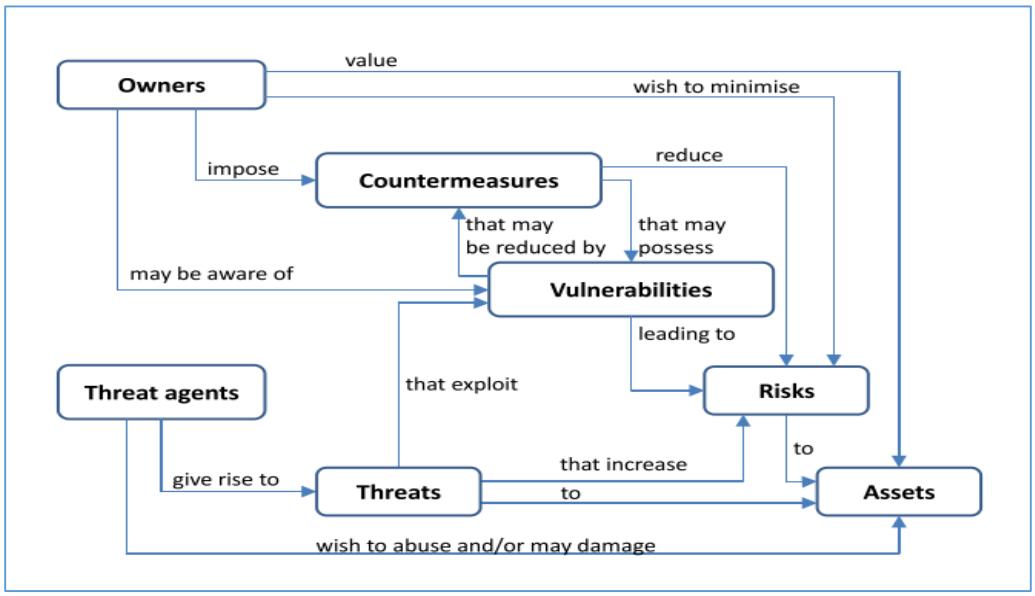


Figure 3.1: Vulnerabilities' Centrality in Information Security (ISO, 2009)

Nonetheless, despite their expectations, Neuhaus and Plattner (2013) have shown that vulnerability fix rates do not decline as time progresses. Adding to that, research on vulnerability discovery has shown that finding vulnerabilities does not conclusively result in overall more secure software (Rescorla, 2005). Those results indicate that vulnerabilities are a given and not something that gradually disappears with system maturity.

What's more, this has been explained using economic terms by various researchers with Ross Anderson being a pioneer in this scientific branch (Anderson & Moore, 2007, 2009; Anderson, 2001; Moore et al., 2009). Major software vendors like Microsoft and Oracle have been trying to create and leverage business ecosystems where they have the role of the central hub or keystone player as this is termed (Iansiti & Levien, 2004). In order to do so, their products need to be attractive to independent developers. Products burdened with security requirements would not have that appeal. Therefore, the mentality of 'ship it now and we will get it right on a later version' prevails. This poses a significant issue since organizations often adapt new technologies in order to remain competitive and drive growth.

All of these, suggest that remediating vulnerabilities is a constant battle. It is also a very important one. Bojanc and Jerman-Blažič report that *"according to the CERT, around 95% of security breaches could be prevented by keeping systems up-to-date with appropriate patches"* (2008a, p. 416).

Additionally, the above facts showcase the added value of a SOC when it comes to vulnerability patching. By being a central point of defense that manages the whole of the ICT infrastructure a well implemented SOC can guarantee that known vulnerabilities will be taken care of in a timely fashion. Moreover, centrally controlled vulnerability management turns system security from a weakest link activity to a best effort one. In other words, the security level of an enterprise as a whole, depends on the efforts of one centralized location and not on the efforts of multiple dispersed ones, where each one of them can be the soft spot that attackers could exploit.

Information Asymmetry

Another factor that heavily influences the information security landscape is the notion of informational asymmetry. The term was first coined in the Nobel prize winning work of Akerlof (1970) and it signifies the imbalance of power that arises in a transaction when one party has more or better information than its counterpart.

Anderson (2001) has used this notion in order to showcase that when it comes to information security the balance of power lies in the side of the attacker. This is derived from the fact that a defender should be able to counter attacks everywhere while an attacker only needs to find a single weak spot. Given that a significant number of previously undiscovered vulnerabilities come to light frequently (for which no patches are available), a huge advantage is given to attackers since they only need to discover one of them to exploit. This information asymmetry is the reason why attacks that take advantage of unknown vulnerabilities (termed zero-day attacks) are considered to be highly dangerous (Peter, 2014).

The extent of the issue can be understood by the fact that organizations like Tipping Point and iDefense exist, with the sole purpose of buying vulnerabilities and forwarding them to their subscribers (Bojanc & Jerman-Blažič, 2008a).

Taking the restrictions above in mind, it can be easily understood that an entirely secure system is not feasible. A SOC however, through its advanced reactionary capabilities, gives the defending organization the opportunity to minimize the damage caused by those attacks by detecting them early on in the kill chain. It can be therefore seen, that by utilizing both its proactive and reactive capabilities, a SOC is able to act as a risk reduction mechanism for the enterprise.

Cyber Insurance Market

One of the most fundamental ways of minimizing the risk under which an enterprise operates is through the insurance industry. However, in the case of the cyber insurance market, the consensus among technology professionals is that it is still evolving and not yet ready to provide organizations with complete solutions (Pearson, 2014). Adding to that, due to the correlative nature of attacks (one exploited vulnerability can cause a worldwide impact) *"cyber-risk markets are [thus] generally uncompetitive, underdeveloped or specialized"* (Anderson & Moore, 2007, p. 69).

This signifies that investments towards information security are currently a one way street for firms that need to operate under a risk reduced environment. Given that, a SOC implementation is an investment that those firms should seriously consider.

Misaligned Incentives

The case of misaligned incentives is one that emerges across multiple parts of the information security spectrum. For example, misaligned incentives have been used to examine information security in critical infrastructures (Anderson & Fuloria, 2010) or the adoption of technical protocols (Clayton, 2010).

In the context of a possible SOC implementation though, the most important observation concerning misaligned incentives is the fact that security systems are particularly prone to failure when their operators are not the individuals that will bear the consequences of those systems failing (Anderson & Moore, 2006). This is especially relevant to large organizations where often a differentiation between the 'guard' and the 'business' entity exists (Walker, 2012). In order to remediate this misalignment a SOC needs to be able to produce repeatable and measurable outcomes in accordance to specified KPIs. Moreover, SOC operators should possess soft skills like an operational excellence attitude and winning mentality.

Probably the most important aspect of misaligned incentives is concerned with SOC outsourcing. Organizations trying to focus on their core competencies often outsource security operations to Managed Security Services Providers (MSSPs). However, MSSPs are not going to be the ones paying for the damage done in case of a security failure. It is therefore of outmost importance that the organizational embedding of a SOC is carefully considered and implemented in a watchful manner.

Information Security Landscape - Conclusion

All of the above clearly indicate that organizations need to prioritize information security. Today's miscreants are well equipped and their motivation has lead them to operate in a professional and industrialized manner. Moreover, it has been shown that vulnerabilities - the soft spots in an organization's defense will keep occurring since software vendors have no real driver for building more secure code. Attackers will therefore be always able to exploit them.

By combining all of these with the current deficiency of alternative risk management solutions such as cyber-insurance a case can be formed. The case that information security should be considered as a foundation of conducting business properly. The regularly used motto of 'it's not a question of whether an organization will be targeted/breached but when' seems to be closer to reality than not.

Additionally, it has been shown that the concept of a Security Operations Center fits well to the current information security landscape in the sense that its capabilities are well aligned to the landscape's current problems. What's more, given that uncertainty seems to be a permanent feature of the information security landscape a SOC can act as a risk reduction mechanism for enterprises.

The Cyber Threat Landscape

The overview of the information security landscape clearly showed why managing the risk deriving from cyber threats should be prioritized in the minds of decision makers worldwide. This section intends to give a higher level description of the means that attackers use in order to achieve their goals. In other words, what kind of cyber-attacks exist, what is their intended impact and who performs them.

The section is structured as follows. Firstly, it presents the types of adversaries that organizations face. Continuing, it gives an overview of the various forms of cyber threats that exist. Adding to that, an overview of attempts to quantify the financial damage of cyber threats is presented.

Types of Adversaries

The cyber domain is plagued by various threat actors or adversaries. Between them, technical skills and motivations significantly vary. The Dutch Cyber Security Centrum (2013) defines various groups of adversaries each of which is analyzed below in terms of motivation and capabilities.

State actors

During the past decade governments have understood the importance of cyberspace (Obama, 2009) and have developed information warfare capabilities (McAffee, 2009). State actors are individuals or groups that work for a country's government. They do so in order to promote the internal and external political agenda of their country's regime. They usually develop offensive capabilities while being extremely technically skilled. Their attacks use multiple methods, are targeted and highly sophisticated.

Their main targets are state and military secrets, intelligence data, as well as threatening the availability of critical infrastructures. The attacks of 2007 in Estonia, 2008 in Georgia as well as several highly publicized incidents are widely believed to have been perpetrated by state actors (Choo, 2011; Hewlett-Packard, 2013). For the sake of completeness, it is worth mentioning that arguments supporting the view that state actors were not the group responsible in the case of Estonia have been raised (Lesk, 2007).

Cyber criminals

Cyber criminals are the most widely known and active group of threat actors. They are financially motivated while certain groups of them possess sophisticated technical skills. Among them exists a relatively small group of specialists possessing extremely high knowledge and expertise. This group is the driver for new cyber-attack developments while cooperation among its members is commonplace (National Cyber Security Centre, 2013).

Independently of their skillset, all cyber criminals have access to the underground market where lately the term 'cybercrime as a service' has come to life. Although being quite self-explanatory, the term suggests that virtually anybody can have access to various specialized threat agents, their expertise and tools. To give an indication, Manky (2013) describes some of the services on offer in the underground market as well as their price:

- Consulting services such as botnet setup: $350 – $400
- Infection services: around $100 per 1,000 installs
- Distributed Denial of Service (DDoS) attacks: $535 for five hours per day during a week's timespan

Those services are only indicative and many others exist like code obfuscation, renting of Command and Control (C&C) panels, and credit card verification and sales (Sood & Enbody, 2013). It is therefore evident that the term cyber-criminal incorporates various types of people who can act under different roles such as buyer, seller or provider of services. Nonetheless, given their motivation and ability, cyber criminals are the most common - if not the most important - adversaries that threaten organizations.

Script kiddies and cyber vandals

Those types of adversaries are distinguished by the fact that their motivation has to do with recognition and pride. Despite the similarity in incentive, a significant discrepancy exists between the technical skills of those two hacking groups. On the one hand cyber vandals are extremely skilled and create their own tools. On the other, script kiddies use tools built by others and have limited technical knowledge thus being a limited threat to enterprises (Aggarwal, Arora, Neha, & Poonam, 2014). Nonetheless, their existence alone, is indicative of the fact that the skills needed to perform hacking activities are decreasing.

Hacktivists

Hacktivists are groups that conduct cyber-attacks for ideological purposes. The most widely noted group of them are Anonymous who since 2012 have been responsible, among others, for the posting of bank managers' online credentials (Blue, 2013) and Distributed Denial of Service (DDoS) attacks on UK, US and Swedish government websites (Dunn, 2012).

While successful attacks by hacktivists reveal that technical skills do exist among them there is a wide variation among the different groups. Nonetheless, an important factor regarding attacks by this group of threat actors, is the fact that they receive a lot of media attention and are widely publicized. This could potentially reduce trust towards attacked firms.

Internal Actors

Insider threats consist of employees, current or former, that due to either ignorance or malicious intent expose firms to cyber risk and/or damage. Their motives exhibit a lot of variation and can range from revenge in the case of disgruntled employees to financial ones in the case of a member of staff that is approached in order to perform corporate espionage. Although most often those threat actors are not technically skilled their knowledge of the organization's structure and possible access to it gives them a significant head start in achieving their goals.

What is interesting concerning this particular group of threat actors is the fact that while attacks involving them are relatively limited in quantity (Verizon, 2012), the damage they deliver is usually higher than attacks perpetrated by external threat actors (PWC, 2014). This is especially important in the light of the fact, that the predominant trend is that organizations *"take very little or no proactive measures to monitor insider threat activity or to reduce the risk of insider activity"* (Pilling, 2013, p. 17).

Corporations

Both the European Union Agency for Network and Information Security (2013a) and the Dutch Cyber Defense Center (2013) concur that corporations constitute active threat actors. Although there is quite a dispersion in the technical skills it is not uncommon for corporations to hire services from other threat actor groups. Their ultimate motivation is of course financial but it is achieved through collecting business intelligence, gathering of confidential information on competitors and breaching intellectual property rights.

Intellectual property rights are an especially important issue with official state reports putting the estimated losses at 21 billion pounds (about 1.8% of GDP at the time) for the UK (Detica, 2011) and over 300 billion dollars for the US (The Commission on the Theft of American Intellectual Property, 2013). However, to mention all the points of view the former report's findings have been doubted by respected researchers on the information security field (Anderson et al., 2013).

Adversaries – Conclusion

From the above, it can be clearly understood that a multitude of threat actors exist with a wide range of capabilities and motivations. Nonetheless, all of them could potentially harm corporations and have a vested interest in doing so. What's more, if we ignore inside group variations most adversary types are in possession of high technical skills. Adding to that, even if they don't possess those skills, the underground market is an efficient way to obtain them and in the case of internal actors they might not even be needed.

Given the multitude of threat actors, enterprises investing in a SOC should build it according to the adversaries that will most probably attack them. For example, firms active in the finance industry should be more focused on attacks perpetrated by cyber criminals than those in the critical infrastructure section. Both of them though should be concentrated on internal actors. This suggests that the technology as well as the processes inside the SOC could be structured differently.

Moreover, it can be seen that many of adversaries have or can be backed by a significant financial background. Given their monetary motivation and the fact that they can sustain longer periods of zero profit, it is logical to assume that targeted attacks (requiring significant time on part of the attacker) will increase in the future. As mentioned previously and contrary to SOCs, point security solution deployment has proven to be ineffective against them. Therefore, organizations that could be pitted against such

adversaries should consider SOC implementations as a countermeasure against them. Lastly, Figure 3.2 summarizes the types of adversaries presented above according to their technical capabilities and expertise.

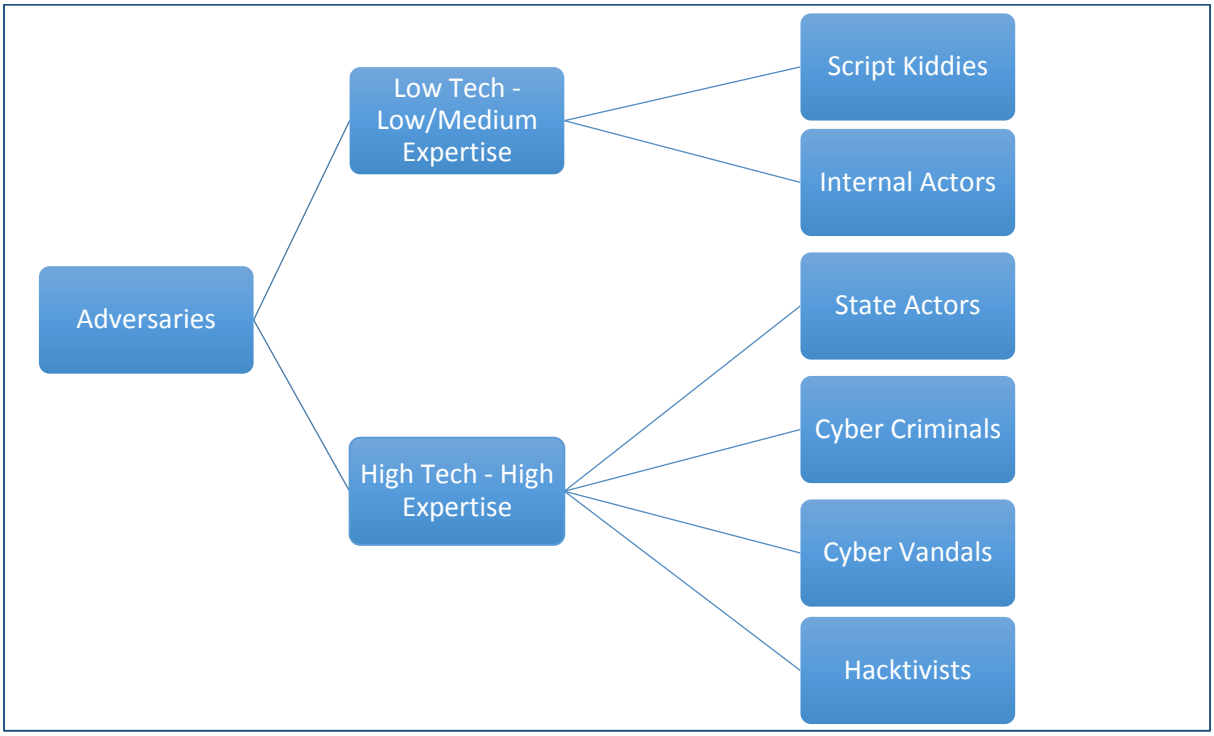


Figure 3.2: Classification of Adversaries

Cyber Threats

This section aims to give an overview of the currently highest profiled cyber threats. Moreover, the kill-chain model proposed by Lockheed Martin researchers (Hutchins et al., 2011) to prototype the steps of Advanced Persistent Threats (APTs) is used, in order to show how those cyber threats are commonly used in such a context. This is done since APTs have been reported to be the ones bearing the heaviest impact on organizations and one of the main advantages of SOCs is that they can either defend against them or at least minimize their impact.

It is important to note that the kill-chain model is not used as a threat categorization mechanism. It is used to showcase the plethora of attack vectors that adversaries have at their disposal when performing an APT attack. The kill-chain consists of seven steps:

1. Reconnaissance: Selection of targets and research about them. The research outcomes include a variety of things ranging from social relationships to information on specific technologies.
2. Weaponization: Implementation of the malicious payload and disguising it under acceptable formats such as PDF files.
3. Delivery: Transmission of the malicious payload to the target environment by various means such as email or portable USB drives.
4. Exploitation: Actual work perpetrated by the malicious payload once it has entered the target's environment. This work is usually performed by exploiting technical vulnerabilities.
5. Installation: This phase has to do with installation of specific software that allows the attacker to have consistent access to the target's environment.

6. Command and Control (C2): The attacker has now full ('hands on the keyboard') access on the infected systems and is able to manipulate them according to his wishes.
7. Actions on objectives: The last phase is the attainment of the actual goal of the whole attack.

The threats are presented in a timeline order from earliest to latest according to the model's phases. This is done by the combined use of a closed chevron process and a threat rectangle. The chevrons represent the model's steps. At the same time the adjacency of the rectangle to the chevrons' position determines a threat's mapping to the model's phases as shown in Figure 3.3.

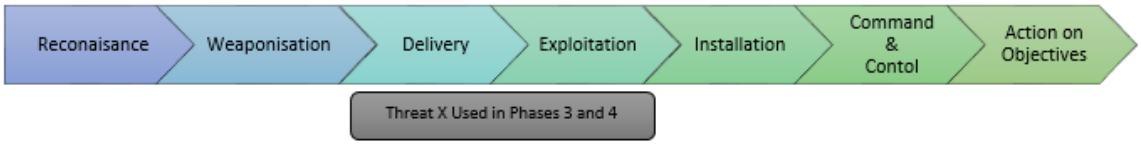


Figure 3.3: Kill Chain Modelling Legend

Phising

Phising attacks are defined as *"online scams that frequently use unsolicited messages purporting to originate from legitimate organizations, particularly banking and finance services, to deceive victims into disclosing their financial and/or Personal Identity Information (PII) to commit or facilitate other crimes"* (Choo, 2011, p. 724).

The usual method that phishing employs, is redirecting unsuspecting users to legitimate looking websites that are designed in such a way that the retrieval of users' information such as login credentials is possible. While phising is typically associated with emails it has also spread to the social media and mobile realms while the methods by which it's implemented have become more complex over the past few years (Kaspersky Labs, 2013).

Additionally, another form of phising has emerged lately. Spear-phising employs the usual phising techniques with one major difference. It is extremely targeted in the sense that it tries harvest information from selected individuals such as the CFOs or the payroll department of organizations. Gordon Snow (2011), an FBI director, has disclosed that spear-phishing was used in cases that involved the actual loss of 85 million dollars.

To give an indication of the problem's size, Moore and Clayton (2007) have deducted that a number between 280,000 and 560,000 individuals fall victims to phising websites each year. Adding to that, Anderson et al. (2013) have estimated that the cost of phising to the global economy was in the area of 320 million dollars. It must be mentioned though that their estimate was based on a, Gartner provided, 'cost per successful phising attempt' figure, that has been doubted afterwards (Florêncio & Herley, 2013). Figure 3.4 shows phishing's positioning on the kill chain.

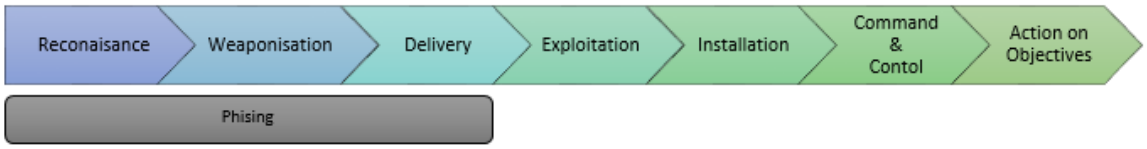


Figure 3.4: Position of Phising in the Kill Chain

Spam

Spam is one of the ways that attackers come to contact with their targets. Spams is usually used in order to deliver malicious software to the target's email or to lure the target into other scams. There are two major

types of spam. Those are email and social spam (Kim, Jeong, Kim, & So, 2011). To give an indication of the volume of spam, according to Symantec (2014), during 2013 66% of all mail traffic over the Internet was spam with an average of 29 billion mails per month. Figure 3.5 shows spam's positioning on the kill chain.

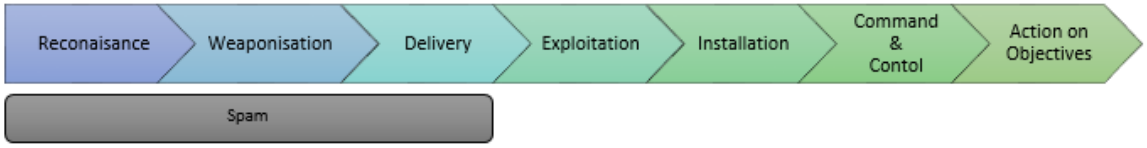


Figure 3.5: Position of spam in the kill chain

Watering Holes

A watering hole can be viewed as a kind of spear-phishing attack in the sense that it targets specific groups of people instead of selected individuals. This is done by manipulating websites that this particular group would regularly visit through the use of malware. According to the US Industrial Control Systems Cyber Emergency Response Team (2013) watering holes have been the initial point of many successful attacks.

What's more, watering holes seem to be increasing in usage by attackers (ENISA, 2013a). This could be seen as evidence that adversaries are focusing their attacks more so as to increase their gains by selecting the right targets. Figure 3.6 shows the position of watering holes in the kill chain.

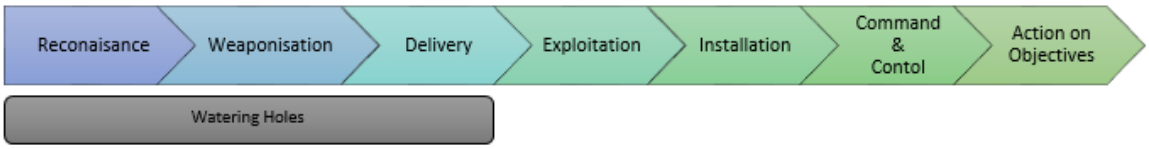


Figure 3.6: Position of watering holes in the kill chain

Drive-by Downloads

Drive-by downloads are automated attacks that occur when a user visits an infected website often referred as a 'malicious URL'. Once the website has been visited the user's computer is automatically scanned for vulnerabilities. If those are detected malicious software is deployed to exploit them.

Adding to that, along with phising, watering holes have been identified as the most important threat to the client side of the financial infrastructure (Hämmerli, 2012). Moreover, they have consecutively been ranked as the number one threat in terms frequency (ENISA, 2013a, 2013b). This is not surprising since browser are the first line of interaction with the Internet and malicious URLs are a prime attack surface. Figure 3.7 shows the positioning of drive-by downloads in the kill chain.

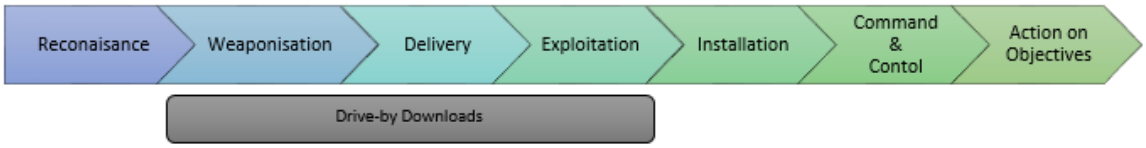


Figure 3.7: Position of drive-by downloads in the kill chain

Code Injection

Code injection is a technique which exploits software vulnerabilities in order to make legitimate software behave in a malicious manner. In technical terms, the most common ways of doing so is by SQL injection, Path Traversal, Cross-Site Scripting (XSS) and Cross-Site Request Forgery (CSRF). By utilizing data withdrawn from the US National Vulnerability Database (2014) Figure 3.8 shows the vulnerability trends concerning those kinds of code injection methods over the past few years. At the same time, Figure 3.9 shows the position of code injection in the kill chain.

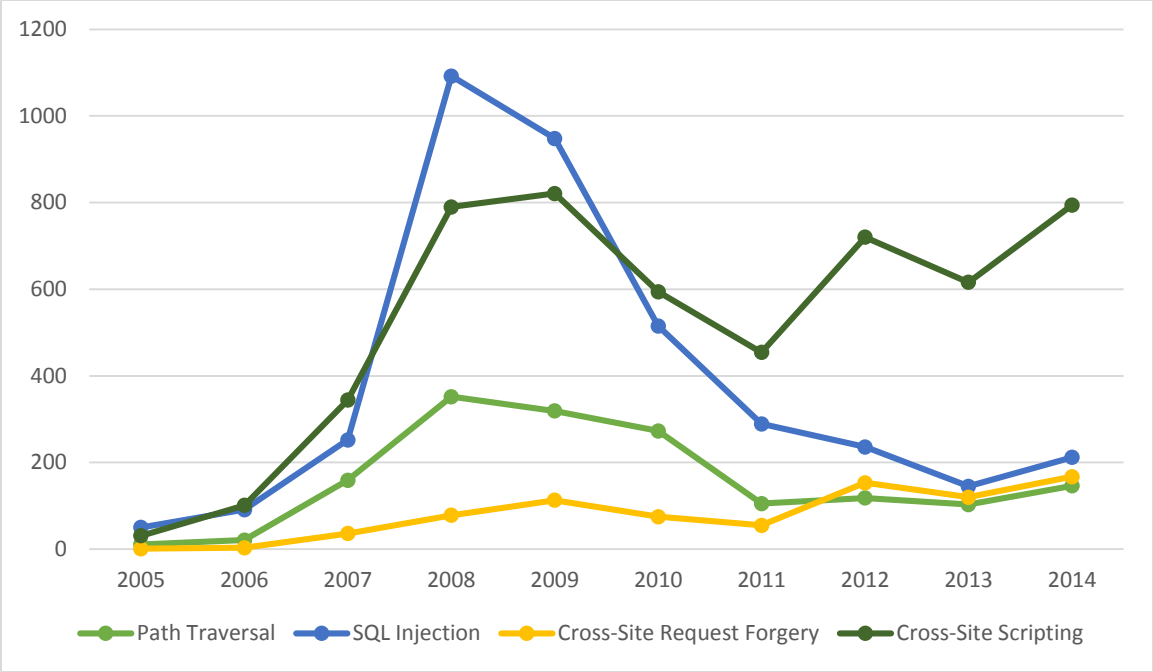


Figure 3.8: Vulnerability trends for common code injection attacks methods

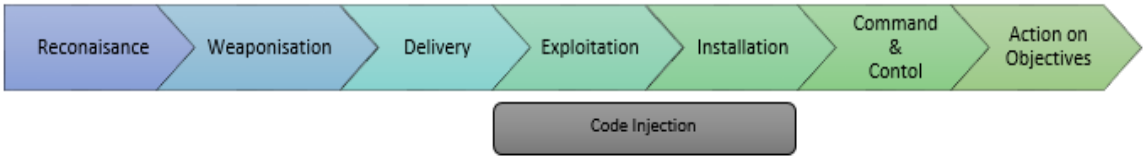


Figure 3.9: Position of code injection in the kill chain

Ransomware

Ransomware is malicious software that demands payment from victims in order to relieve them of its presence. Usually this was done by utilizing a fake authority scam which would normally not be of interest in a SOC context. Since 2013 though, the fake scam has been abandoned for more effective methods. An exemplary case is Cryptolocker that restricted access to computer files by encrypting them with very strong encryption techniques (US CERT, 2013).

Traditionally, methods to extract money from victims did not include ransom tactics since it was difficult for criminals to extract the money. The emergence of anonymous payment channels though, has solved this issue for cybercriminals and has driven the increase of ransomware (F-Secure, 2014; Mcafee, 2013; Symantec, 2014). Figure 3.10 shows ransomware's positioning on the kill chain.

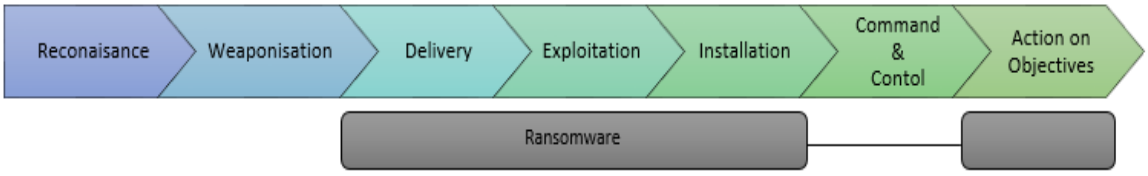


Figure 3.10: Position of ransomware in the kill chain

Exploit Kits

Exploit kits are one of the main tools of attackers. They are software packages specifically designed to rapidly identify and attack computer vulnerabilities. There are two distinct characteristics concerning

exploit kits and their ecosystem. Firstly, not only can exploit kits be bought in underground cyber-markets but a customer support relationship exists after the sale has been made (ENISA, 2013a; Malecki, 2013). This suggests that exploit kit users and developers are two distinct threat groups.

Secondly, Kotov, and Massacci (2013) by analyzing the source code of more than 30 different exploit kits came to the conclusions that they were independently written and that commercial code protection mechanisms were embedded on them. Those facts suggest an active and profitable exploit kit development ecosystem. Figure 3.11 shows the position of exploit kits in the kill-chain.

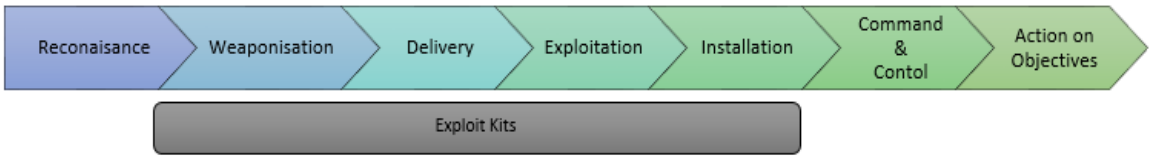


Figure 3.11: Position of exploit kits in the kill chain

Worms and Trojans

According to ENISA, worms and trojans are the second most frequent type of threat (2013b). They are both types of malicious software with distinct characteristics. On the one hand worms have the ability to replicate themselves across networks, thus automatically infecting multiple systems. On the other, trojans hide into other legitimate programs and reveal their true intent only when activated (Rainer, 2008). The payload they carry varies and could be anything ranging from file encryption to creation of backdoors used to access the infected system on a later stage (Kim et al., 2011). Figure 3.12 shows their position on the kill chain.

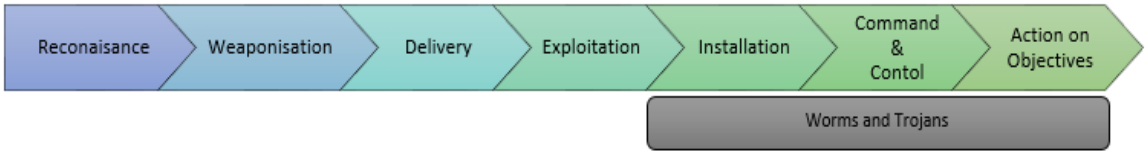


Figure 3.12: Position of worms and trojans in the kill chain

Botnets

Botnets constitute a network of infected machines each of which can act according to the wishes of the attacker that infected them, often referred to as 'botnet herder'. The size of the network can often be in the millions of infected nodes. To give an example, the Conflicker botnet that was used to attack the French Navy and Ministry of Defense, was comprised of 15 million infected computers (Robinson, Gribbon, Horvath, & Robertson, 2013).

Botnets can be seen as the infrastructure of cybercrime since they *"provide a versatile platform for a variety of criminal business models, including sending spam, committing click fraud, harvesting account credentials, launching denial-of-service attacks, installing scareware and phishing"* (Anderson et al., 2013, p. 288). Figure 3.13 shows the position of botnets in the kill-chain.

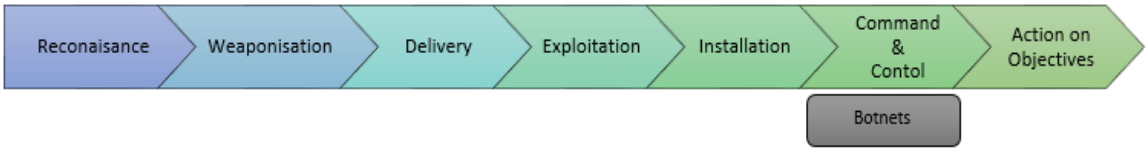


Figure 3.13: Position of botnets in the kill chain

Denial of Service (DoS)

Denial of service attacks have as a target to disrupt the normal operations of IT systems most notably by crippling their connectivity. The most commonly used variant of DoS attacks is the distributed one. A Distributed Denial of Service (DDos) uses the same principles as the normal one but is launched from hosts scattered across the Internet typically leveraging a botnet (Douligeris & Mitrokotsa, 2004).

DDoS attacks have increasingly been targeting data centers over 2013 (Arbor Networks, 2014) and have also been reported to be used in order to influence market values and interfere with exchange platforms of the financial industry (Akamai, 2014). Adding to that, they have been used as a diversion when another more significant attack is taking place (Krebs, 2013).

Figure 3.14 shows the position of DoS attacks on the kill chain. It must be mentioned that thought not apparent here the major part of a DoS attack should be positioned on the last phase of the kill chain (Action upon objectives).

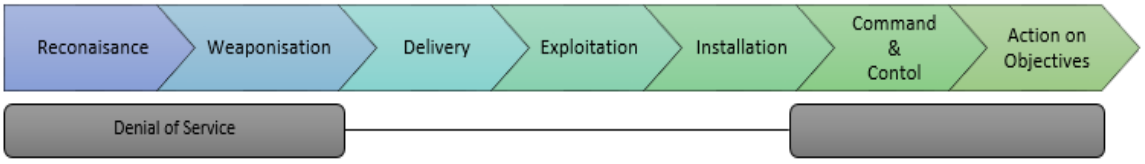


Figure 3.14: Position of Denial of Service in the kill chain

Advanced Persistent Threats (APTs)

APTs are distinguished by the fact that they are extremely targeted and occur over a wide timeframe. Moreover, they are characterized by persistence meaning that the attacker is not willing to switch targets in the face of difficulties. In terms of the technical methods used, APTs can be thought of, as a combination of the threats mentioned above. Moreover, they have shown to routinely bypass traditional security countermeasures (Potts, 2012; PWC, 2014)

Targeted cyber-attacks have been used to both perform cyber espionage and steal intellectual property as was the case of operation Aurora in 2009 and disrupt the functionality of critical infrastructures as was the case for Stuxnet in 2010 (Sood & Enbody, 2012). Figure 3.15 shows the position of APTs in the kill chain.

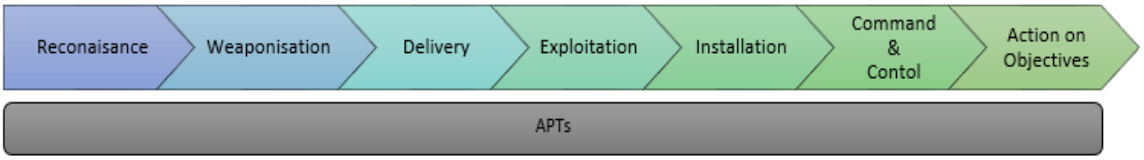


Figure 3.15: Position of APTs in the kill chain

Cyber Threats Costs

What has been presented so far, concerning the cyber threat landscape, clearly establishes that multiple cyber threats exist, perpetrated by various actors that usually possess advanced technical skills. Moreover, the information security landscape shows that issues deeply rooted within the domain of cyber security aid threat actors to continue on their missions and cyber threats to be successful.

Given these and in order to complete the cyber threat landscape, it is essential that the impact of successful attacks needs to be measured. This is vital so that organizations can clearly assess the dangers they might face and act accordingly. However, such an assessment has proven to be a daunting task for both academia and industry for a multitude of reasons.

Various reports have attempted to present data concerning the cost of security failures. However, the reader should be very skeptical when drawing conclusions from this data. This is due to two reasons. The first is that organizations tend not to report successful attacks against them. There are several reasons pertaining to that, like the beliefs that either incidents are not serious enough or that the chances of successful prosecution are very limited. The most important cause though is the fear of loss of customer trust and the competitive disadvantage that derives from negative publicity (Richards, 2009). Therefore the data are probably incomplete. Adding to that, data tend to be over or underestimated according to who collected them (Anderson et al., 2013). For example, security vendors might augment the perception of threats in order to gain more clients. This kind of bias threatens the integrity of data.

The data that are presented below are drawn from two industry reports and a scientific paper. The first set of reports are authored Ponemon Institute that has been conducting yearly researches on the cost of data breaches (Ponemon Institute, 2013, 2014). The reports take into account both direct and indirect costs of data breaches which is very significant. Moreover, the findings are divided among several countries. On the other hand it must be mentioned that they were sponsored by active stakeholders in the information security field (Symantec in 2013, IBM in 2014). Figure 3.16 shows the average cost of a data breach according to the Ponemon results.

The second report is one conducted by PwC and commissioned by the British Department for Business Innovation and Skills. The authors surveyed a sample of 1098 UK companies of all sizes. The main finding was that the average cost of the worst security breach for large organizations ranged from 600k to 1.15m pounds and from 65k to 115k for small firms (Department for Business Innovation and Skills, 2014).

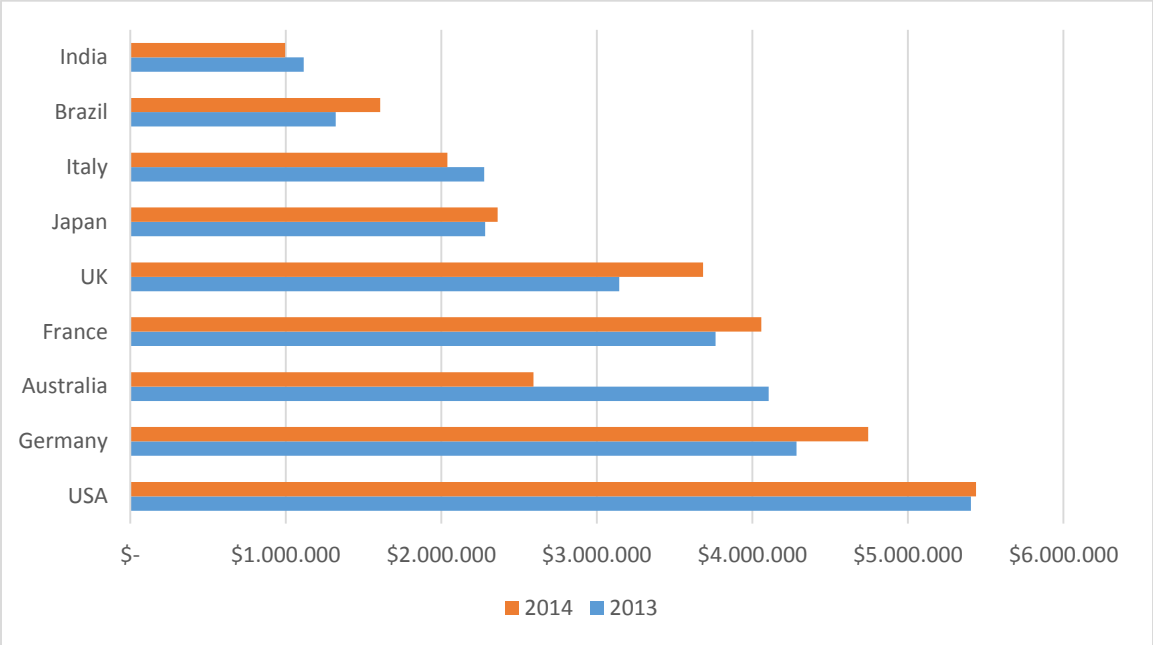


Figure 3.16: Average cost of a data breach per country (Ponemon Institute, 2013, 2014)

Lastly, Anderson et al. (2013) have performed a study to determine the impact of cybercrime on a UK and global scale. They have done so by either scaling down or up in accordance to the respective GDPs. Their findings however sometimes do not include indirect costs and sometimes the authors warn of under or overestimations. Table 3.1 summarizes their findings relevant to a possible SOC implementation.

Type of Cybercrime	UK Estimate	Global Estimate	Reference period
Online banking fraud – phising	$16m	$320m	2007
Online banking fraud – malware	$6m	$300m	2010
Online banking fraud – Countermeasures	$50m	$1000m	2010
Online payment card fraud	$210m	$4200m	2010
Offline payment card fraud	$373m	$7440m	2010
Loss of confidence (consumers)	$700m	$10000m	2010
Loss of confidence (merchants)	$1600m	$4960m	2009

Table 3.1: Cost estimations for various types of cybercrime (Anderson et al., 2013)

Chapter Conclusion

Given all of the above there are three main conclusions that can be drawn. Firstly, by looking at the information security landscape it easy to understand that the dynamics that are able to spawn cybercrime are and will most probably remain existent. Software vulnerabilities for example will not stop to exist since software vendors have no real interest in eliminating them while at the same time, threat actors that wish to exploit them have little reason to fear they will be caught for doing so.

Given those dynamics an escalation of the dangers to information security seems to be a very probable scenario. Taking into account the fact that point security solutions seem to have reached their individual potential, the need for appropriate responses on the organizations' side seems not only imminent but also essential. A SOC, with its advanced threat detection and prevention capabilities, could be the medium implementing those responses thus enabling firms to perform 'business as usual' in a risk reduced environment.

Secondly, a multitude of actors exist that have a vested interest to perform cybercriminal activities. Moreover, they can do so while having the support of an established market dedicated to cybercrime. At the same time a vast repertoire of methods to perform their actions is at their disposal. Organizations should therefore be able to defend against threats spanning across this repertoire's spectrum.

Properly implemented SOCs can offer better protection against individual threats by streamlining the remediation of security gaps. Moreover, complex attacks like APTs that combine multiple attack methods can be spotted early on in the kill chain, thus having their inflicted damage minimized by properly defined remediation processes.

Lastly, the ambiguity concerning cybercrime costs brings organizations to an admittedly uncomfortable position. If those costs have been reported correctly they are not negligible to say the least. If not, the uncertainty factor that this introduces to the conduction of business is not to be disregarded either since their risk management is bound to perform sub-optimally due to incalculable input factors.

All in all, the facts of the security status quo lead organizations to appreciate that developing proper information security practices is not optional or just an added cost on the balance sheet. It should be considered as the toll to pay for entering and remaining competitive in the market.

Having considered all of the above the substantial investment required to build and operate a SOC can be viewed from a different perspective. This perspective should be more about what is the optimal amount to be invested in order to minimize risk and less on whether or not to do so.

Chapter 4 – Security Operation Center Business Benefits

The previous chapters have illustrated how SOC capabilities can improve the information security competences of organizations as well as the complexity and hostility of the information security environment. This chapter completes our proposed SOC business perspective by presenting the business drivers that could underline a possible SOC implementation.

Those business drivers have been derived as the direct outcome of relating the insights drawn from the other two building blocks of our business perspective to the results of a literature review focused on two main axes. Those axes were the impact of successful information breaches on organizations and business benefits of information security. The results of this endeavor are presented in the following sections.

Market Valuation Preservation

The previous chapter illustrated why the costs impacted by an information security incident are proving hard to quantify. In order to overcome those obstacles academia has adopted an indirect but rather pragmatic way of assessing those costs. This is by observing abnormal fluctuations on a firm's market price after that firm has publicly disclosed a successful breach of its systems. The methodology used by academia is the event study one (Craig MacKinlay, 1997; McWilliams & Siegel, 1997) in conjunction with the semi strong efficient market hypothesis (Fama, 1970). The methodology suggests that the stock market assesses public information concerning a firm and incorporates them into its stock value. This is done within a time frame of a few days, usually after new information are made public. This time frame is known as the event window or event period.

In their study, Garg, Curtis and Halper (2003) examined a sample of publicly traded companies with an average market cap of $86 billion. They showed that an average loss of 5.6% occurred on the companies' share price over a three day period after a security incident publication. They also found out that the most severe market reaction pertained to credit card information theft.

Examining a similar period to the aforementioned study but focusing on DoS attacks Hovav and D'Arcy (2003) came to the conclusion that the market does not penalize firms that experience such attacks. It must be noted that the authors used a relatively small sample size (23 samples) compared to the requirements of the event study methodology (over 200). They also came to the same conclusion on a study focusing on virus attacks and using a much bigger sample (Hovav & D'Arcy, 2004). It must be nonetheless mentioned, that virus attacks by their very nature break the hypothesis of independency. This hypothesis is a fundamental aspect for the proper use of the event study methodology.

Additionally, Campbell, Gordon, Loeb and Zhou (2003) found significant negative impact on firms' stock value after disclosure of attacks related to the unauthorized access to confidential data. They however, could not report a significant relationship when it came to different types of attacks. This is not the case on the study of Cavusoglu, Mishra and Raghunathan (2004) where an average negative impact of 2.1 per cent on market value – independent of the type of security incident - was found. Given their sample this could be also translated to an average damage of $1.65 billion in market capitalization.

A study performed by Gatzlaff and McCullough (2010) utilized a data set consisting exclusively of breaches relating to unauthorized access of personal data. Their sample consisted of 77 firms. They show that over a two day period exposed firms experienced an average damage of 0.84 per cent in their stock price. Given the median value of firm market capitalization in their sample this relatively small percentage corresponds to *"a loss of $84 million in market value for the median-sized firm"* (Gatzlaff & McCullough, 2010, p. 75). Moreover, firms that were perceived as unforthcoming in sharing breach related information seemed to be more heavily penalized by the market.

Two studies relating to the subject at hand that can be considered as complimentary are the ones performed by Gordon, Loeb and Zhou (2011) and Pirounias, Mermigas and Patsakis (2014). They can be viewed as such since they both use the exact same methodology and the latter examines a time period starting at the former's respective period's end.

What's more, both of those studies use both the – previously extensively utilized - Capital Asset Pricing Model as well as the Fama-French three factor model in order to calculate abnormal returns on stock value. Moreover, the authors provide solid argumentation as to why the latter produces more accurate results. Both of the studies find a significant negative impact publicized successful on firms' stock value. The results are even more statistically significant when the Fama-French model was utilized.

Using the aforementioned model Gordon et al. (2011) find negative impact on the stock market value statistically significant on the 1% level. Additionally, Pirounias et al. (2014) observe abnormal returns ranging from 0.15 to 0.39 per cent depending on the event window used. The reader should not be influenced by the relatively small percentages since *"the average total cost of a security breach [] is estimated to be in the range of $168-$200 million"* (Pirounias et al., 2014, p. 169).

Table 4.1 summarizes the major studies performed on the subject. The event period observed is indicated by a [X,Y] form where X represents the first day studied and Y the last. A zero indicates the day an incident has been made public. If the result was negatively statistically significant the respective event window is bolded.

Year	Author(s)	Time Span	Sample Size	Event Window(s)
2003	Garg, Curtis & Halper	1996 – 2002	22	**[0,3]**
2003	Campbell, Gordon, Loeb and Zhou	1995 - 2000	43	**[1,1]**
2003	Hovav and D'Arcy	1998 - 2002	23	[1,0], [1,1], [1,5], [1,10], [1,25]
2004	Hovav and D'Arcy	1988 - 2002	224	[0,0], [0,1], [0,5], [0,10], [0,25]
2004	Cavusoglu, Mishra and Raghunathan	1996 - 2001	66	**[0,1]**
2010	Gatzlaff and McCullough	2004 – 2006	77	Multiple, ranging from [-5,0] to [0,180]; **([0,1] to [0,35])**
2011	Gordon, Loeb and Zhou	1995 - 2007	121	**[-1,1]**
2014	Pirounias, Mermigas and Patsakis	2008 - 2012	105	[-1,1], **[-1,0]**, **[0,0]**, [0,1]

Table 4.1: Summary of studies concerning cyber-attack disclosure and market valuation

Event studies have also been used in order to evaluate whether various kinds of investments in information technology have caused an increase on the stock valuation of firms (Dehning, Richardson, & Zmud, 2003; Im, Dow, & Grover, 2001; Ranganathan & Brown, 2006; Sabherwal & Sabherwal, 2005).

Chai, Kim and Rao (2011) have performed this kind of research when it comes to information security investments. Using a sample of 101 enterprises they have come to three conclusions. The first was positive cumulative abnormal returns ranging from 1.01 to 1.89 per cent on the firms' stock price. Secondly, they established that investments with the aim of commercial exploitation were treated more generously by the market compared to those for IT capabilities improvement. Lastly, that the implementation of the Sarbanes-Oxley act had a positive impact on the aforementioned returns.

Given all of the above, a relationship to SOCs becomes apparent. Firstly, a SOC can protect enterprises from security incidents and their costly aftermath by preventing them from happening in the first place. Secondly,

despite a SOC implementation being a costly endeavor for a major enterprise it is only a fraction of the impacted costs discussed previously. Therefore, part of this investment could be at least partially justified by the expected abnormal returns on the firm's stock price.

Moreover, the fact that many of the aforementioned researches found a significant impact on stock price when incidents disclosed related to personal information, signifies that SOCs, should prioritize the defense of assets containing such information. Additionally, in order to minimize the impact from undefended incidents a SOC should be able to leverage pre-existing relationships with the public relations department of the organization or offer media relation capabilities of its own (Zimmerman, 2014). Additionally, a predetermined action plan must be set in place when disclosures need to me made (Kulikova, Heil, van den Berg, & Pieters, 2012).

Lastly, the very recent developments in the European Union's legal framework concerning data privacy (European Comission, 2014) strengthen both of the above SOC related arguments. More specifically, enterprises will most likely have to timely report even on possible privacy breaches (European Comission, 2012). This suggests that the risk on firms' stock value is greater as well as the tactic of avoiding disclosure becomes a highly disputable option.

Additionally, a fine of up to 2 per cent of the worldwide turnover of an enterprise could be imposed given that the enterprise does not adhere to certain information security practices (European Comission, 2012). This is especially important from a stock valuation perspective since it has been shown that markets penalize more heavily information security breach announcements that impact a firm's bottom line.

Information Security Investment Optimization

Despite its advantages, complete information security can be a prohibitively costly endeavor for an enterprise. This is why enterprises have moved from what is optimal to what is economically feasible (Anderson, 2001). Moreover, justifying information security investments is often referred as the most challenging aspect of information security projects due to the nonfunctional character of security. This is why often the strategy of promoting fear, uncertainty and doubt (FUD) has often been utilized in order to support such projects (Al-Humaigani & Dunn, 2003; Berinato, 2002; T. Tsiakis & Stephanides, 2005).

In order to solve this problem as well as estimating the optimal amount of investment, both academia and industry have come with multiple information security investment models. Different approaches exist in literature that can be categorized according to the method and metrics they use.

The first major category (Al-Humaigani & Dunn, 2003; Bojanc & Jerman-Blažič, 2008a, 2008b; Derrick Huang et al., 2008; Mizzi, 2010; Purser, 2004; Sonnenreich, 2006) utilizes one or a combination of evaluation metrics such as Return On Investment (ROI), Return On Security Investment (ROSI), Net Present Value (NPV) and Internal Rate of Return (IRR).

The second category employs approaches originating from finance or economics such as real options pricing (Derrick Huang et al., 2008; Gordon & Loeb, 2002; Hausken, 2006; Willemson, 2010) or combining rent-seeking theory with production economics (Hausken, 2012). Other approaches utilize risk-based return (Arora, Hall, Piato, Ramsey, & Telang, 2004), value-at-risk (J. Wang, Chaudhury, & Rao, 2008) and game theory (Cavusoglu, Mishra, & Raghunathan, 2005; Gao, Zhong, & Mei, 2013).

Independently of their origins all of these approaches have a common denominator. Their underlying requirements assume knowledge of specific information pertaining to the security posture of the organization. This knowledge includes:

- Probability of an attack against assets
- Annual loss expectancy from successful attacks

- How efficiently a security investment reduces the probability of loss
- The sum of vulnerabilities in information systems

Such knowledge however is proving difficult to come by. Many attacks go unnoticed (Böhme & Moore, 2013; Hyman, 2013; National Cyber Security Centre, 2013; Whitman, 2003) and actuarial data are not available due to firms' disposition not to share occurred security incident specifics (Cavusoglu et al., 2004; Chai et al., 2011; Hyman, 2013). This lack of hard data leads to a garbage in – garbage out conundrum when applying those approaches. This is why some of them have been criticized (Wood & Parker, 2004) as practically infeasible.

A SOC however is able to detect many of the attacks that often go unnoticed due to its technological capabilities (Hewlett-Packard, 2009) as well as due to the fact that it serves as a centralized entity that handles information security incidents throughout their complete lifecycle (Koivunen, 2012). Taking that into account, a SOC can leverage its knowledge of the organization's infrastructure as well as its external partnerships in order to confidently assess attack probabilities as well as the fit and efficiency of possible information security controls.

The previous chapter illustrated why information security is no longer an option as well as the fact that investments in it will be common practice onwards into the future. We have seen however the difficulties in optimizing those investments which suggests that many of them are being made with argumentation based on fear and uncertainty rather than solid facts.

A SOC can provide the risk management function of the enterprise with the data needed in order to perform its role. This will inevitably lead to security investment, cost optimization. Additionally, the fact that benefits derived from the information security function will be quantifiable will enable it to be perceived as a business enabler and not as just a non-functional requirement and cost.

Brand Strength, Trust and Reputation Preservation

Brand equity is considered the most important intangible asset of a firm (Aaker, 2009; Neumeier, 2005) since it allows enterprises to generate higher profits (Ailawadi, Lehmann, & Neslin, 2003; Leuthesser, Kohli, & Harich, 1995). Inextricably woven into brand equity are the notions of brand strength, brand trust, and brand reputation (Aaker, 2009; Delgado-Ballester & Luis Munuera-Alemán, 2005).

Over the past decade a significant proliferation of cyber-attacks has been observed. Headlines have been filled with such news (Emm, 2013; Nkhoma, Jahankhani, & Mouratidis, 2007) and therefore public awareness concerning them has been raised. The lack of trust towards information security that this awareness brings along, has often been cited as an inhibitor to the adoption of several business initiatives such as B2C e-commerce (Pavlou, Liang, & Xue, 2007) or internet banking (Cheng, Lam, & Yeung, 2006). This of course translates to lost business opportunities.

What's more, brand strength and reputation can be severely impacted by a successful attack against a firm (Hyman, 2013; Kulikova et al., 2012). This means that consumers might choose to stop being loyal to an impacted firm and switch to competition. Equally important to the perception of consumers is the opinion of other entities in the firm's value chain.

An emblematic case is the so called mega-breach at retailer TJX Companies Inc. where the firm in question had to make financial settlements with banks, credit unions, clearing houses and processors as well as credit card companies and issuers in order to maintain its credibility as a business partner (Hovav & Gray, 2014). Perhaps all of the aforementioned facts can be summarized in IBM's (2013) finding, that the average reputational costs of a severe IT operations disruption is almost $5.3 million.

All of the above indicate that information security is linked to brand equity through brand strength, trust and reputation. In order to enhance the latter and achieve higher purchase intentions, organizations have been investing in standardization with successful results (Wu & Jang, 2013a, 2013b). Additionally, a certified firm can be perceived as a safer business partner (Disterer, 2013).

Given that a SOC forms the basis of information security in an enterprise it can actively contribute to brand strength, trust and loyalty. This is performed in a variety of ways. Firstly, it defends firms against cyber-attacks that could damage a firm's brand reputation. Secondly, it enables business initiatives by enhancing trust through its role as a guarantor of customer security and privacy. This is especially important since Vinhas Da Silva and Faridah Syed Alwi (2008) determined that security and privacy have a direct positive impact to online corporate image. Thirdly, a SOC's services (Carnegie Mellon University, 2014) directly align with various information security standards such as the widely accepted ISO 27 family of standards.

Cost Avoidance

Probably the most important business driver behind a SOC implementation is cost avoidance. The previous chapter has shown that despite the fact that reported costs vary a lot they are not insignificant and introduce a substantial amount of uncertainty in business operations.

Costs incurred from cyber-attacks are also varying in nature. They can be impacted from:

- Downtime of systems that leads to missed business opportunities (S. Wang, Zhang, & Kadobayashi, 2013)
- Regulatory fines (Anderson et al., 2013)
- Market valuation reduction as explained above
- Theft of intellectual property (The Commission on the Theft of American Intellectual Property, 2013)
- Loss of consumer and business partner trust (Ryan, Mazzuchi, Ryan, Lopez de la Cruz, & Cooke, 2012)
- Legal action initiated by consumers, employees or business partners (Shackelford, 2012)
- System remediation activities and countermeasure deployment (Anderson et al., 2013)

All of the impacted costs have an information security breach at their core. A SOC can actively contribute to the diminishing of those costs by either not letting those breaches occur or minimizing their likelihood and impact. Additionally, given that breaches will occur (no system is completely safe) a SOC's forensics function can aid the enterprise in the possible ensuing legal procedures.

The notion of cost avoidance can also be linked to new business ventures. The approach that information security should be directly linked to new projects is adopted by industry (Harkins, 2012), academia (K. T. Tsiakis & Pekos, 2008) as well as by the developing regulatory environment. An example of the latter, is the legislation being passed by the European Commission (2014) that enforces data protection by design and default. Given its knowledge of an enterprise's infrastructure as well as its security expertise a SOC can actively contribute to upholding the requirements of this emerging paradigm.

Lastly, a special mention should made about regulatory compliance. Indeed, regulatory fines have a significant effect on an organization's bottom line (Q1 Labs, 2009). Another significant cost however is related to the effort of proving compliance. When it comes to it though, a number of industrial case studies have shown, that the technical capabilities of a SIEM system (a technological component ever-present in SOCs) significantly reduce the effort needed as well as the impacted costs (Hewlett-Packard, 2011b; RSA Security, 2009).

Increased Investor Confidence

By combining all of the above another business benefit of a SOC implementation can be surmised. The impression that the presence of a well implemented SOC leads to increased investor confidence. This comes as a consequence of several facts.

Firstly, investors do not observe abnormal fluctuations of stock value due to successful cyberattacks and subsequent disclosures. Secondly, a SOC can serve as evidence of proper IT governance especially if its reporting capabilities allow it to provide stakeholders with relevant reports (Stoll, 2013).

Lastly, a SOC can be considered as an investment in IT slack as this is defined in the work of Rahrovani and Pinsonneault (2012, p. 170): *"[The] cushion of actual or potential IT resources that allows IT or organizational adaptation to internal and external pressures and jolts"*. This consideration should be based on the uncertainty that currently dominates the information security and cyber threat landscapes in conjunction with the SOC's advanced response capabilities. The same goes for the increasing regulatory environment. All of the above are in accordance with the notion of business resilience which in turn leads to increased investor confidence.

Chapter Conclusion

A SOC can actively provide significant business benefits to a firm. Firstly, by eliminating threats before they occur or minimizing their impact a SOC protects a firm's stock value from abrupt drops. This capability also contributes to the preservation of brand equity since both customers as well as business partners perceive the firm as trustworthy. Moreover, a firm can leverage the SOC in order to make informed decisions that will lead to optimal resource allocation. Additionally, financial benefits are derived by several types of cost avoidance. Lastly, it has been surmised that all of the above lead to increased investor confidence. Table 4.2 maps the aforementioned business benefits to SOC high level goals as those were described in the second chapter of this thesis.

Business Benefit	High Level SOC Goal
Market Valuation Preservation	Threat control and/or prevention
Information Security Investment Optimization	Situational awareness deliverance
Brand Strength, Trust and Reputation Preservation	Threat control and/or prevention
Cost Avoidance	Threat control and/or prevention, Forensics, Risk and/or downtime reduction, Diminishing of administrative overhead, Audit and compliance support
Increased Investor Confidence	Threat control and/or prevention, Audit and compliance support, Risk and/or downtime reduction

Table 4.2: Business benefits and SOC goals mapping

A SOC Business Perspective

The current information security environment has been shown to be not only complex but also hostile towards organizations. A conjecture of facts heavily benefits organizations' adversaries that have substantial financial motives underlying their actions. Not only are those adversaries in possession of high technical expertise but they also have a relative freedom of action given the law enforcement's inability to keep up with them.

Additionally, the current information security situation does not appear to be likely to change. The way the software market operates suggests that the existence of software vulnerabilities will remain an unsolved issue thus giving the balance of power to the attackers' side due to information asymmetry. Additionally, the cyber security industry operates in a lemon market manner thus making it difficult for organizations to optimize their value for money ratio when it comes to information security investments.

Lastly, the costs of cybercrime introduce a high amount of uncertainty and risk to the conduction of day to day business. Uncertainty, that the cyber insurance market is not mature enough to shield firms from yet. All of the above suggest that organizations both need to be proactive about protecting themselves as well as the fact that significant business benefits can be drawn from doing so.

In their own turn, those benefits are both hard as well as soft ones. They involve a multitude of cost avoidance facets ranging from remediation activities and lost business opportunities to legal and regulatory fines. Additionally, market valuation preservation can protect the monetary capital of firms. Lastly, brand strength protection and increased investor confidence can also be derived from enhanced information security.

At the same time, conventional point solution approaches are proving to be inadequate in protecting organizations. On the contrary, due to their advanced capabilities stemming from the orchestration of security solutions, SOCs can adapt better to the contemporary information security environment thus enabling organizations to reap the business benefits of enhanced information security and conduct business in a diminished risk mode.

This is possible since SOCs have the ability to streamline the remediation of software vulnerabilities across the organization. Moreover, SIEM systems, being a SOC's technological backbone have the capacity to detect security incidents that would otherwise go unnoticed. Something especially important given the multitude of attack vectors modern cyber threats, increasingly employed by adversaries, such as ATPs utilize.

To do so SOCs utilize a sizeable database of security related information, finding correlations among its different records. This database can be further used in order to support the organizational efforts pertaining to compliance and audit preparation.

What's more, information security spending is and will remain a one way street for organizations. Due to their technical expertise and coordinated approach towards information security SOCs can optimize the investment in technology security solutions. Moreover, they can provide real-world data to the risk management functions of organizations thus enabling them to perform their role without the fear of their models misrepresenting reality due to input of poor quality.

To summarize, SOC goals and capabilities appear to be perfectly aligned to the requirements dictated by the current information security environment. Consequently, SOCs are capable of enabling organizations to reap the benefits stemming from superior information security. All of the above, are graphically depicted in Figure 4.1 that presents our SOC business perspective.

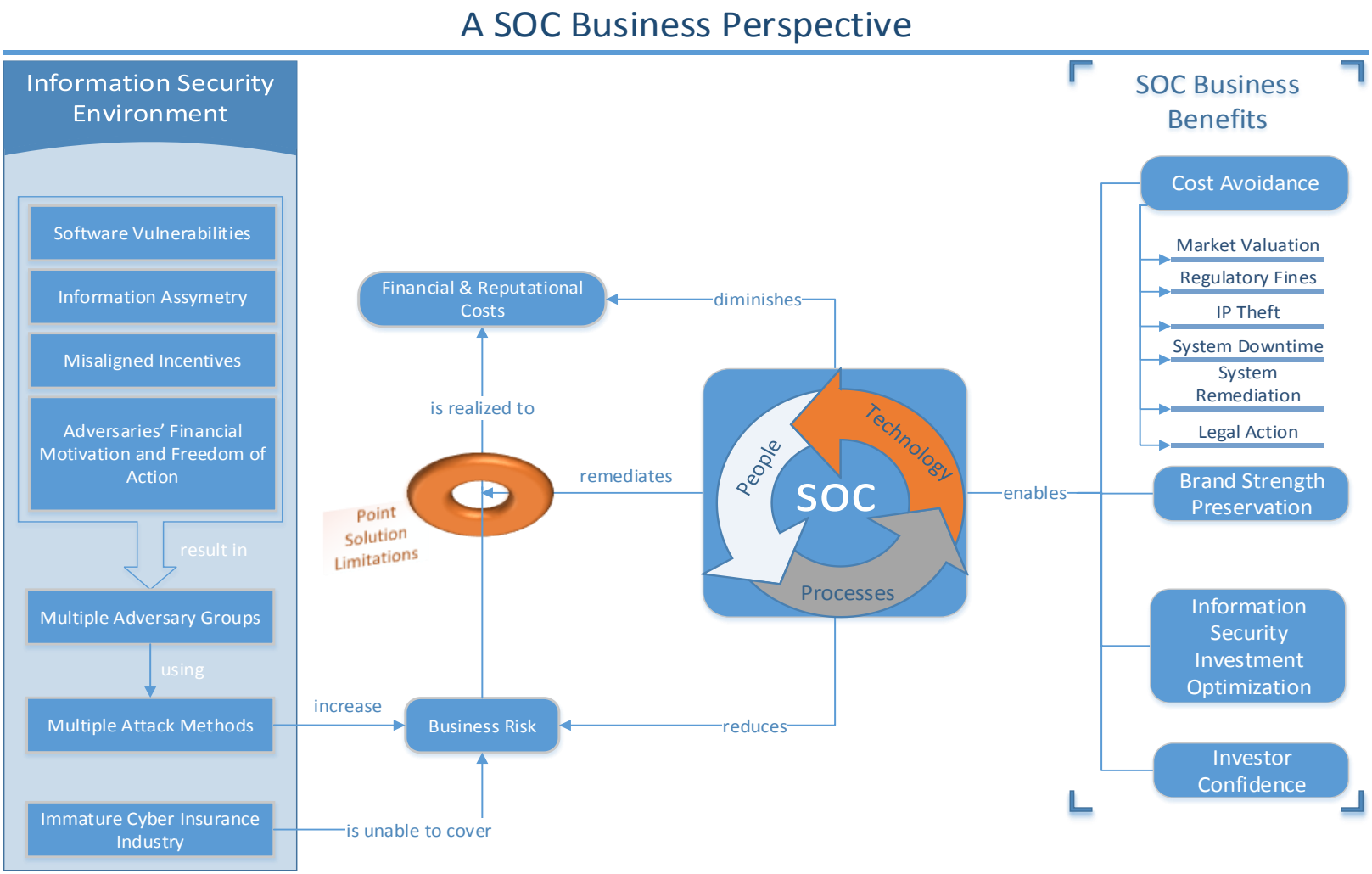


Figure 4.1: A SOC Business Perspective

Chapter 5 – Improved Threat Control Testing

Introduction

Our SOC business perspective has displayed that SOC goals and capabilities are indeed well suited to face the adversities of the contemporary information security landscape thus enabling organizations to reap a variety of business benefits.

It is highly noteworthy, that closer inspection of Table 4.2 reveals that threat control and prevention is the SOC goal almost all of the identified business benefits are related to. Nonetheless, to the best of the author's knowledge there are no scientific studies that have tested whether SOCs indeed deliver on their promise of increased information security organizational performance through enhanced threat control and prevention.

This means that while our business perspective indicates that SOC investments should be strongly considered by executive decision makers, there is no empirical foundation for these investments to be based upon. Therefore, scientifically backed evidence of superior SOC performance on threat control and prevention would cement our business perspective.

This chapter describes the steps that were undertaken to answer this thesis' second research question which is related to the aforementioned issue. To give a reminder this was:

RQ2: *Does the existence of a well-established Security Operations Center lead to better organizational performance concerning information security when it comes to the hacking, card fraud, and insider data breach types?*

In order to answer our question the approach of statistically confirming that well established SOCs indeed offer their constituencies enhanced threat control and prevention was chosen. Given that information security is defined as *"protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction []"* (United States Government, 2013, p. 148) in the context of our statistical testing we can establish a cognitive link between threat control and prevention and enhanced organizational information security performance.

Thus, since our selected approach involves statistical methods there is a need to quantify the concept of enhanced threat control and prevention. The first thing that needs to be understood here is that the concept of threat prevention is inherently unquantifiable. This stems from the fact that if an information security failure has not occurred at an organization it can be attributed to two reasons. Either an attempt against the organization was made and failed or the attempt never happened in the first place!

The concept of threat control however can be quantified. To do so, a dataset of information security data breaches that have occurred over the past 10 years has been utilized. The amount of records breached is measurable at the interval scale and can be used as a metric of whether an organization responded effectively against an attack aimed at it. In other words, whether a better organizational performance was achieved when it comes to threat control and information security by extension.

In Chapter 2 we saw that SOCs can vary in terms of organization and capabilities. To achieve internal consistency across the SOC sample we used the members of the unambiguously accepted Forum for Incident Response and Security Teams (FIRST).

By drawing data from FIRST two fundamental requirements are being covered. The first is that this enables us to know with certainty that a breach occurred despite the presence of a SOC. The second is that the SOC in question was well established since becoming a FIRST member entails the successful evaluation on set of

predefined criteria. Those criteria are evaluated by an onsite visit and are shown in Table 5.1 (Forum of Incident Response and Security Teams, 2014). It is important to note that the criteria cut across all three of the technology, people, and process aspects of SOCs. This further supports the argument that the SOCs in question are well established. More information on FIRST members and their constituencies are provided on Appendix B.

General items	Policies	Workplace and environment	Incident handling	Contact information and information dissemination	Professional development
Mission statement or charter	Information classification	Physical security and facilities	Incident reporting procedure	Internal vs. external contact information availability	Training
Document of creation, effective start date, and announcement	Information protection	Equipment	Incident Handling Process	---	Conferences
Defined constituency	Record retentions	Storage	Acknowledging report	---	---
Defined and advertised set of services provided for the constituency	Record destruction	Incident creation / tracking	---	---	---
Funding model	Information dissemination	Network infrastructure	---	---	---
Organizational Home	Access to information	Use of PGP or Identity Management Technology	---	---	---
Team organization in relation to parent organization	Appropriate usage of CSIRT's system	---	---	---	---
---	Computer Security Events and Incidents Definition	---	---	---	---
---	Incident handling policy	---	---	---	---

Table 5.1: FIRST Membership Evaluation Criteria (Forum of Incident Response and Security Teams, 2014)

Lastly, in order to control for the number of records that a malicious actor would have access to, a matched pairs sampling method was used. Since the sampling process forms an integral part of our statistical analysis it is described in great extent later on in this chapter.

The rest of this chapter is structured as follows. Firstly, the data collection method that has been used is described. Continuing, the data cleansing processes applied on the dataset as well as the composition of the resulting data are introduced. Afterwards, the method used to match organizations with and without a SOC as well as its results are described. Lastly, the results of both a parametric and a non-parametric test that have been used in order to test our hypothesis are presented.

Data Collection

The data used for our statistical tests have been drawn from Privacy Rights Clearinghouse (PRC). PRC is a non-profit organization that consolidates information concerning cyber security breaches in the United States. Those information pertain, among others, to the organizations that were involved in a data breach, its type (e.g. hacking, insider malpractice etc.), the number of records breached as well as its time and place.

PRC draws information mainly from the Open Security Foundation's DataLossDB.org. It is important to note that the DataLossDB.org database has been previously used in the past for scientific research purposes (Lee, Kauffman, & Sougstad, 2011; Pirounias et al., 2014) and is thus appropriate to use in this context. Additionally, Privacy Rights Clearinghouse acquires data from the Databreaches.net website, the Personal Health Information Privacy database and the National Association for Information Destruction.

It is important to note that the Privacy Rights Clearinghouse is only concerned a) with data breaches occurring in the United States and b) with data breaches involving the access to personally identifiable information. This kind of breach has been consistently reported as the most cost intensive for enterprises both in terms of stock price drops (Campbell et al., 2003; Cavusoglu et al., 2004) as well as in terms of overall costs inflicted (Ponemon Institute, 2013, 2014).

The next step was to establish which of those data breaches occurred despite the presence of a well-established SOC. As mentioned before, in order to do so, a secondary dataset has been drawn consisting of the members of the Forum of Incident Response and Security Teams (FIRST) based on the US. Its information were combined with those of the primary dataset in order to achieve our goal.

Initial Dataset Cleansing and Composition Description

The dataset that was obtained, consists of 4.508 data breach listings starting from the year 2005 with a cutoff point for the purposes of this thesis set at the 4th of April 2015. Each listing contained the following information:

- Date of public announcement of the data breach
- Organization(s) impacted by the data breach
- The industry the organization belongs to
- Location of the organization
- Type of data breach
- Number of personally identifiable records breached (if known)
- Short data breach storyline

The first data cleansing manipulation to be performed on the dataset was the removal of duplicates. The criteria that had to be adhered to in order for two listings to be considered duplicates were:

1. The listings should have been publicly announced at the same month and year.
2. The organizations involved should have been the same in both listings.
3. The listings' description and breach type should have been the same.

A handful of duplicate listings was discovered resulting in a dataset of 4491 records.

Before moving on some abbreviation conventions are introduced to the reader that will be used throughout the analysis of the data. Those abbreviations are employed only in charts and figures and in order to enhance their readability. The first concerns the type of data breach while the later the type of industry that the organization to which the breach occurs belongs to. Table 5.2 and Table 5.3 summarize those conventions pertaining to data breach and industry type.

Data Breach Type Abbreviation	Abbreviation's Meaning	Description
DISC	Unintended Disclosure	Sensitive information posted publicly on a website, mishandled or sent to the wrong party via email, fax or mail.
HACK	Hacking / Malware	Electronic entry by an outside party, malware and spyware.
CARD	Payment Card Fraud	Fraud involving debit and credit cards that is not exclusively accomplished via hacking.
INSD	Insider	Someone with legitimate access intentionally breaches information - such as an employee or contractor.
PHYS	Physical Loss	Lost, discarded or stolen non-electronic records, such as paper documents
PORT	Potable Device	Lost, discarded or stolen laptop, PDA, smartphone, portable memory device, CD, hard drive, data tape, etc.
STAT	Stationary Device	Lost, discarded or stolen stationary electronic device such as a computer or server not designed for mobility.
UNKN	Unknown	Unknown cause of data breach

Table 5.2: Data Breach Type Abbreviations Used

Business Type Abbreviation	Abbreviation's Description
BSF	Financial and Insurance Services
BSR	Retail / Merchant
EDU	Educational Institutions
GOV	Government and Military
MED	Healthcare / Medical Providers
NGO	Nonprofit Organizations
BSO	Other Businesses

Table 5.3: Industry Type Abbreviation Used

The insightful reader will notice that not all of the data breach types can be related to the capabilities and scope of a Security Operations Center as those were described in Chapter 2. For example the loss of paper records or mobile computers is something that a SOC cannot protect an organization from. In the context of this thesis three types of data breaches are considered SOC relevant. Those are the hacking/malware, credit card and insider ones. All of the other data breach types are deemed to be SOC irrelevant. This distinction is going to be utilized in all of the statistical tests to follow.

Having all of the above covered and moving to the composition of the acquired dataset Figure 5.1 summarizes the initial dataset's distribution according to the type of data breach while Figure 5.2 does the same per industry. Continuing Figure 5.3 combines the previous two figures to give a more comprehensive picture of the initial dataset.

A first noteworthy observation is that out of those 4491 breaches only 157 pertained to an organization with a FIRST member SOC. Before any rash conclusions are drawn though it is important to note that at the time being there is not a large amount of firms that have an organization-embedded SOC in place.

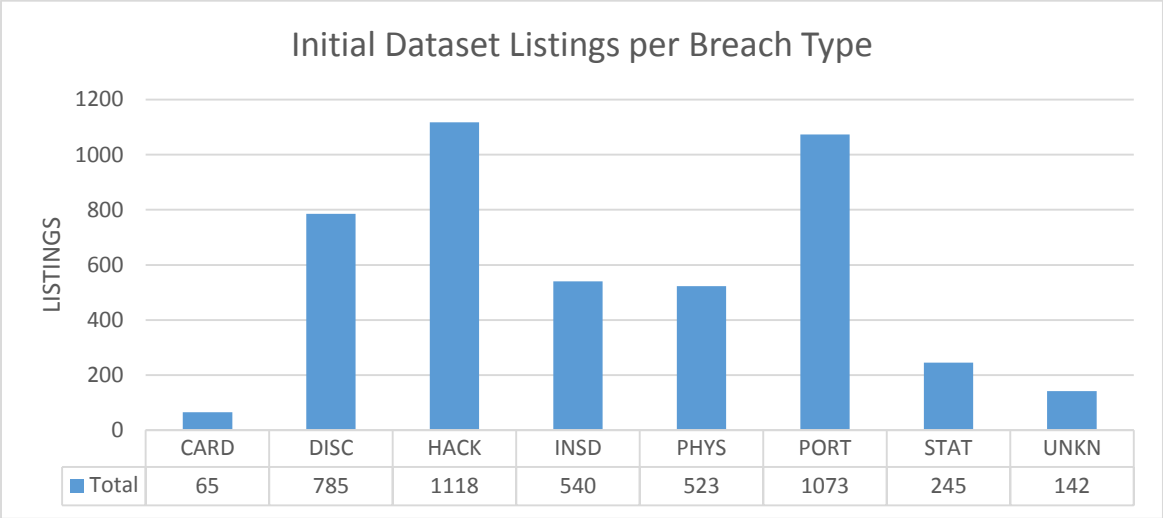


Figure 5.1: Initial Dataset Composition According to Breach Type

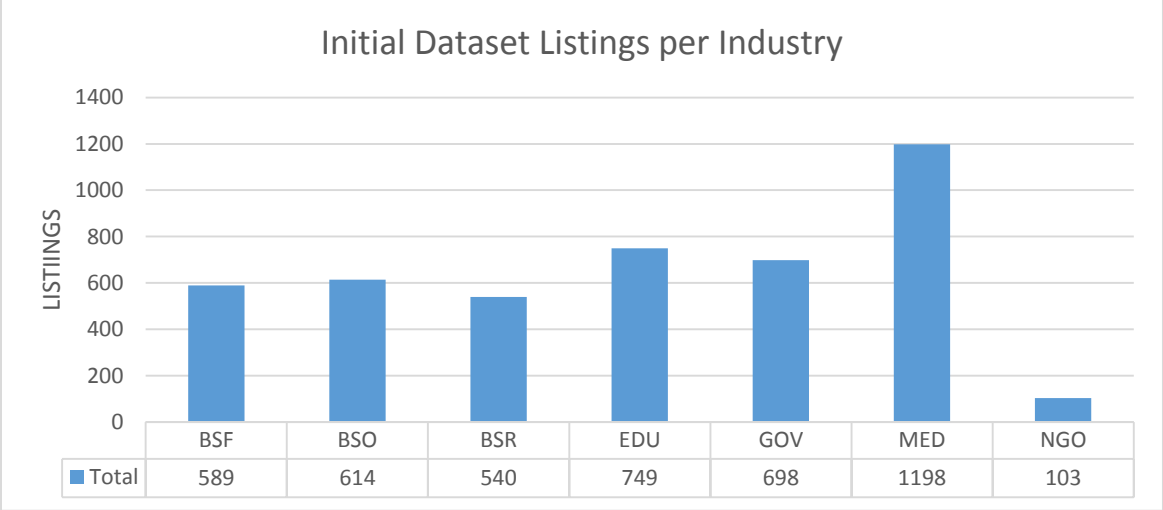
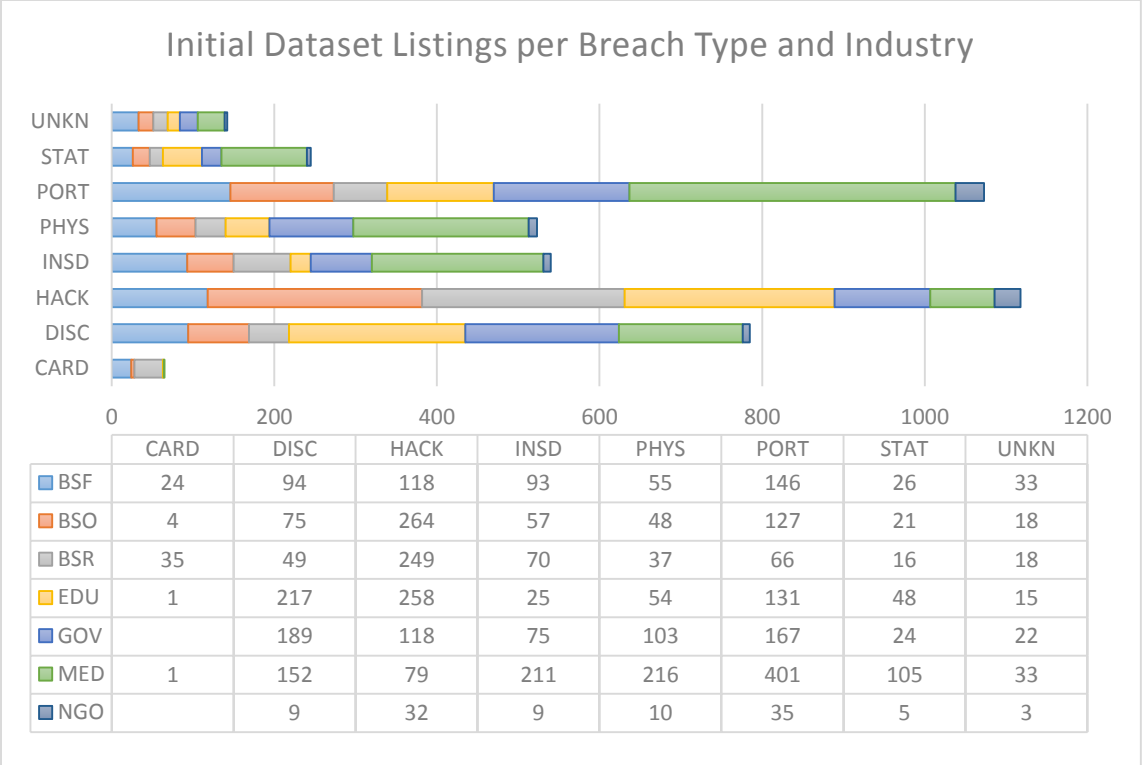


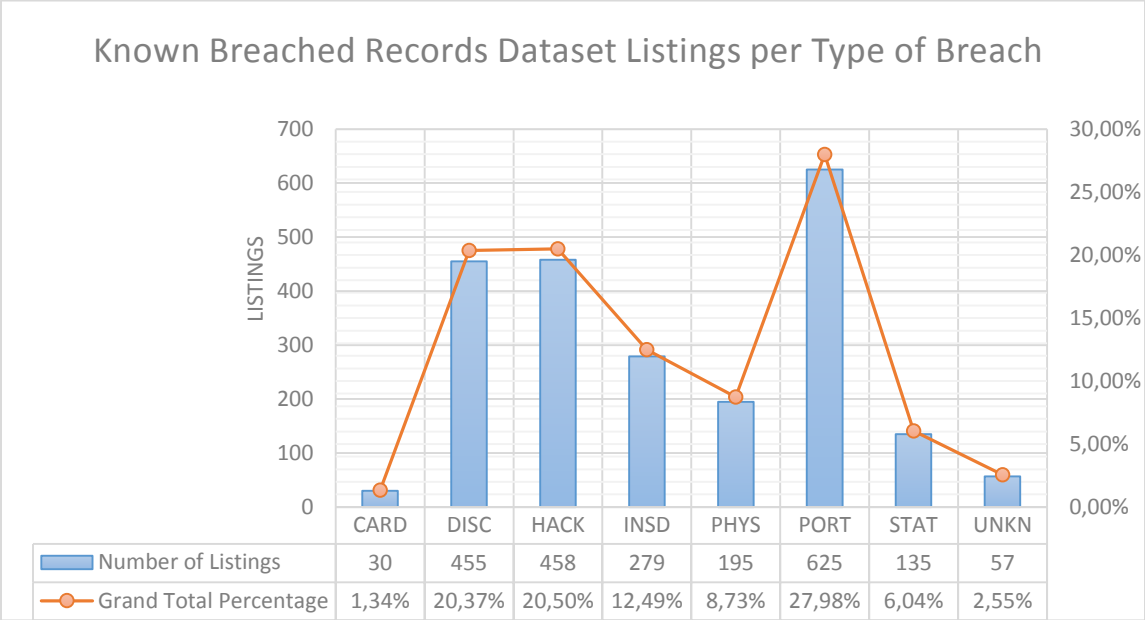
Figure 5.2: Initial Dataset Composition According to Industry Type

The second manipulation on the dataset was to exclude breaches that did not include a known number of records improperly accessed. Thus a dataset of 2230 listings was formed. Figure 5.4 shows the manner in which the known breached listings were distributed per type of breach. Figure 5.5 shows the manner in which the listings with known number of records breached were distributed per industry.



	CARD	DISC	HACK	INSD	PHYS	PORT	STAT	UNKN
BSF	24	94	118	93	55	146	26	33
BSO	4	75	264	57	48	127	21	18
BSR	35	49	249	70	37	66	16	18
EDU	1	217	258	25	54	131	48	15
GOV		189	118	75	103	167	24	22
MED	1	152	79	211	216	401	105	33
NGO		9	32	9	10	35	5	3

Figure 5.3: Initial Dataset Composition According to Industry and Data Breach Type



	CARD	DISC	HACK	INSD	PHYS	PORT	STAT	UNKN
Number of Listings	30	455	458	279	195	625	135	57
Grand Total Percentage	1,34%	20,37%	20,50%	12,49%	8,73%	27,98%	6,04%	2,55%

Figure 5.4: Listings With Known Amount of Recorcds Breached per Breach Type

A first interesting insight can be drawn by contrasting, per breach type, the amount of listings (Figure 5.4) to the amount of records breached. The latter is shown in Figure 5.6. As can be seen while the hacking type of breach accounts for 20.5% in terms of listings within the database it also accounts for an impressive 67.85% of records breached. Given that this type of attack is the one that a SOC is first and foremost concerned with this is especially important.

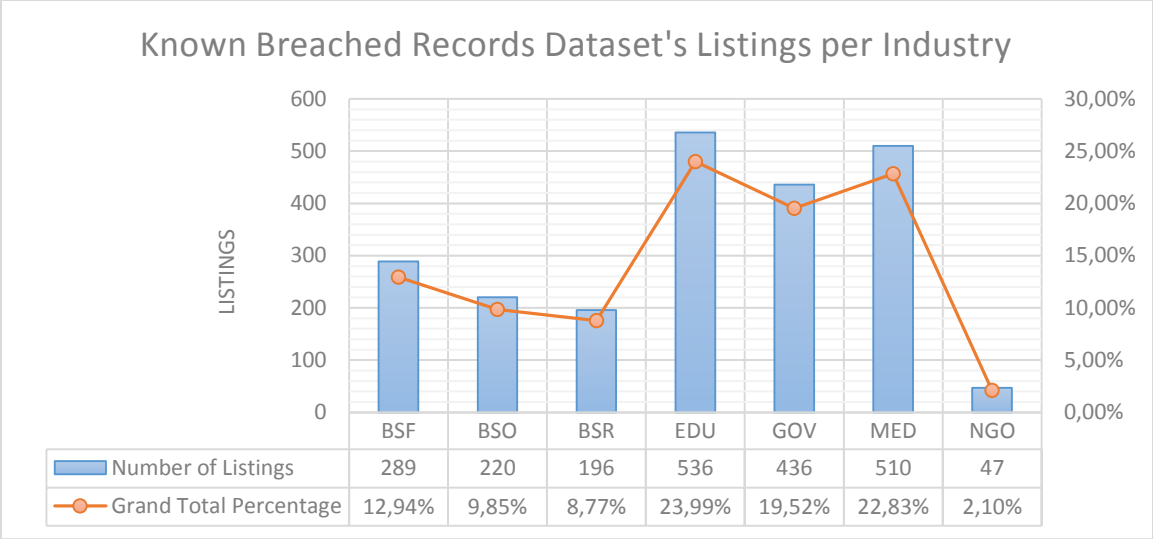


Figure 5.5: Listings With Known Amount of Records Breached per Industry

Another interesting insight that can be drawn from this initial observation of the dataset is the fact that the amount of records breached varies greatly per industry. While the finance industry represents a 12.94% in terms of dataset listings it also accounts for a 41.45% in terms of records breached. The same holds for the retail industry which accounts for 8.77% in terms of listings but represents a 31.56% in terms of records breached. Figure 5.7 illustrates the total amount of records breached per industry.

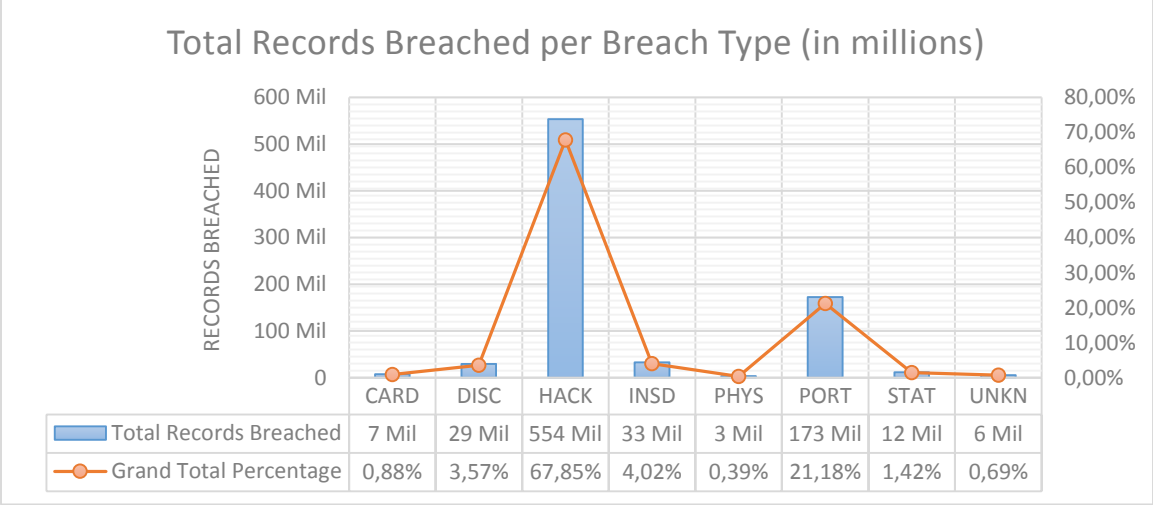
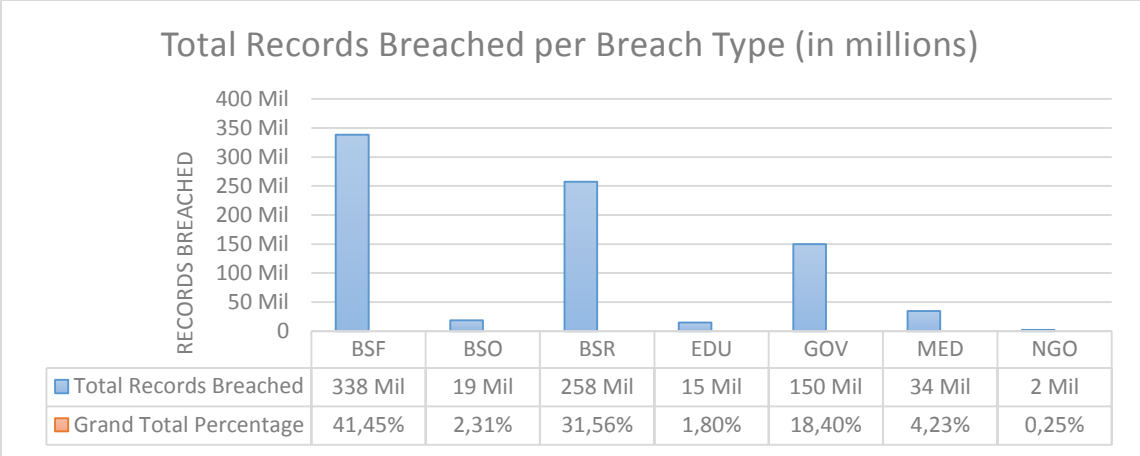


Figure 5.6: Total Records Breached per Breach Type (in millions of records)

This suggests that a breach in those industries is more costly than in other sectors. Given the above it is noteworthy to look on how the types of breaches are dispersed within those two industries in terms of records improperly accessed. Figure 5.8 summarizes this. Within those two industries hacking is the most prevalent accounting for 79,75% and 99,04% within the finance and retail sectors respectively. Figure 5.9 summarizes the same data for the remaining industries.



	BSF	BSO	BSR	EDU	GOV	MED	NGO
Total Records Breached	338 Mil	19 Mil	258 Mil	15 Mil	150 Mil	34 Mil	2 Mil
Grand Total Percentage	41,45%	2,31%	31,56%	1,80%	18,40%	4,23%	0,25%

Figure 5.7: Total Records Breached per Industry (in millions of records)

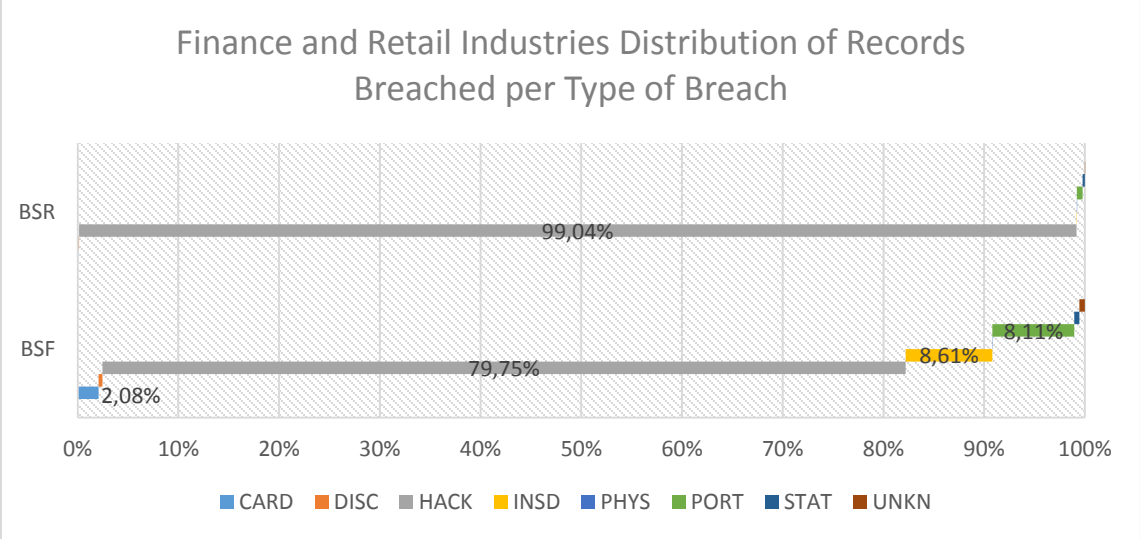


Figure 5.8: Finance and Retail Industries Distribution of Records Breached per Breach Type

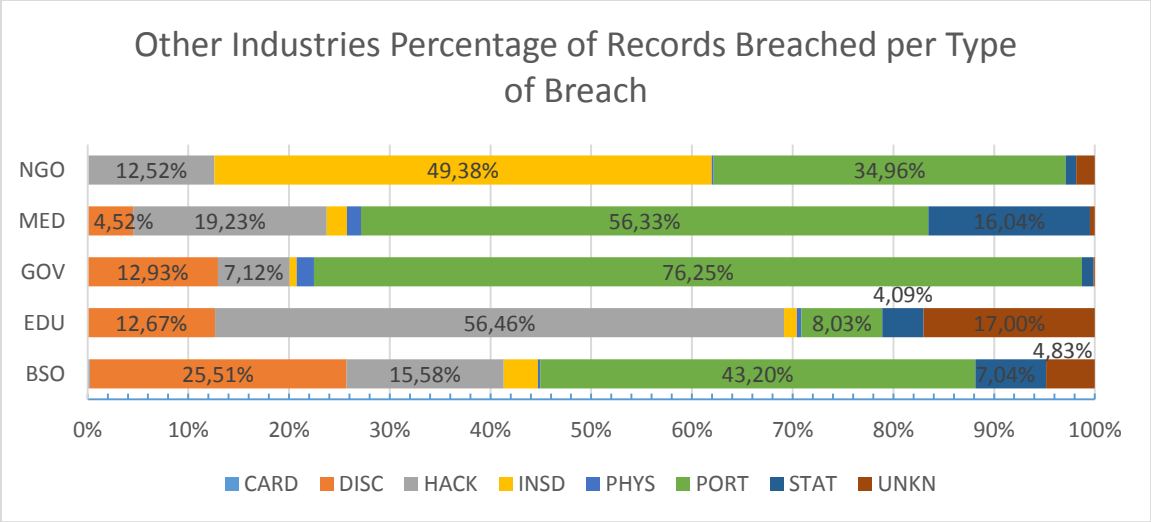


Figure 5.9: Distribution of Records Breached per Breach Type on Non-Financial and Non-Retail Industries

Organizations with an embedded SOC within the dataset

As mentioned previously the dataset was thoroughly searched for breach listings that occurred despite the presence of a SOC appointed to guard the underlying organization. In total 157 such listings were spotted. Among those listings 69 included the number of records stolen.

The listings with unknown breach type (4 in total) were researched in order to determine whether additional information could be found. This resulted in one breach in the US Department of Energy to be moved to the HACK category according to the official report pertaining to it (U.S. Department of Energy, Office of Inspector General, & Office of Audits and Inspections, 2013).

Figure 5.10 shows the distribution of those listings per breach type and industry.

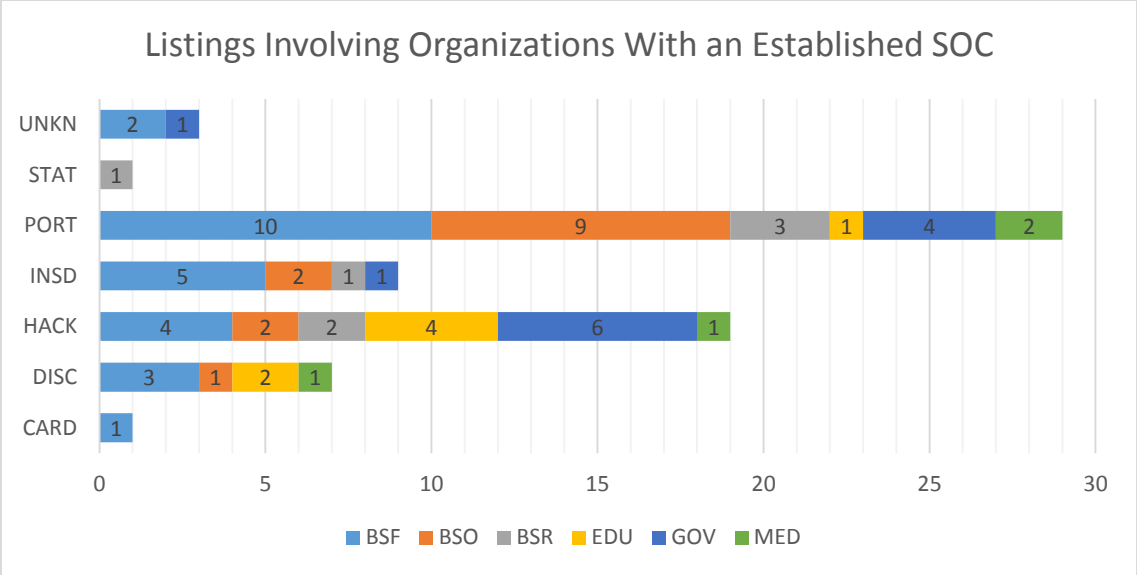


Figure 5.10:Listings Involving Organizations With an Established SOC

The listings pertaining to data breach types (portable/stationary devices, accidental disclosure. and unknown) that a SOC could not relate to were then dismissed to result in a dataset consisting of 29 listings. This dataset was then used as the basis for the test employed to determine whether, in terms of records breached, SOCs provide better protection to organizations than not. The next section describes the procedure followed.

Matched Pairs Process Description

To answer our research question the listings of organizations with and embedded SOC were matched with other listings involving organizations without one. The logic behind this is based on the fact that given the selected approach, the dependent variable on all of the tests would be the amount of records breached. It was therefore essential that:

1. The organizations compared exhibited similar qualities in terms of size and complexity
2. The breaches that occurred exhibited similar characteristics.

Following, the general requirements that had to be adhered to in order for a matched pair to be made are described.

General Requirements

In order for a pairing to be formed the first requirement set was that type of breach had to be the same in both occasions. If this requirement could not be adhered to a pairing was not made and the SOC listing was dropped from the dataset to be formed. Additionally, the organizations involved in each pairing should belong to the same or comparable industries. What's more the organizations should be of similar magnitude and preferably direct competitors.

Moreover, the disclosure date of the breach was taken into account and data breaches occurring at the same year were prioritized over similar ones occurring in different years. This requirement however was considered secondary compared to the one demanding organizations of similar complexity. The rationale underlying this choice relates to the target variable which is the total number of records breached.

To give an example it would be unwise to make a pair concerning a successful hacking attempt between organizations such a Citibank or Bank of America and a smaller bank when one of those banks direct competitors had also been breached at a different but reasonably close year.

Moreover, when a perfect match for a SOC listing could not be found the particular listing was either dropped from the comparison or a selection of an organization by default smaller than the SOC's was made. The underlying logic was that if the subsequent test could prove significant even in such a case the finding would not be arguable.

Lastly, when multiple matches could be found within the database the finally selected one was determined by a random process. This process constituted of counting the possible matches and drawing a random number between 1 and the match count using Microsoft Excel's RANDBETWEEN function.

In order for the pairings to adhere to those requirements different strategies were employed depending on the industry of the organizations participating in the pairings. This strategies are illustrated in the following subsections. Lastly, all of the pairings made and the rationale underlying them are described in detail in Appendix C.

Education Industry Pairings

Two entities having a SOC were found within the educational industry. Those were the Northwestern and Ohio State universities. In total there were four breaches pertaining to them, all of which of the hacking type. Moreover, all the breaches involved records containing personally identifiable information of students, faculty members and staff.

Therefore, in order to determine appropriate pairings it was important to find universities with similar grand totals of student and faculty population size. To do so the Forbes magazine list describing the 650 most respectable universities and colleges of the United States was scrapped. Thus, a secondary dataset was formed containing university names, student body size and student to faculty ratios. The total university population was derived by using the simple formula

$$University\ Population = Student\ Body\ Size + \frac{Student\ Body\ Size}{Student\ Faculty\ Ratio}$$

After all university populations had been calculated four cut off points were set equal to plus/minus 15% of the populations of the two aforementioned universities. Those are shown in Table 5.4.

University	Total Population	Minimum Cut Off	Maximum Cut Off
Northwestern University	24245	20608	27881
Ohio State University	59354	50450	68257

Table 5.4: Population Cut Off Points for Possible Matches of SOC Embedded Universities

Those cut off points were then used in order to search for other institutions similar in population size that had also been breached the same year. If no such matches occurred the search was chronologically extended. If no matches were found despite the extension the SOC based listing was dropped. Fortunately, this was not the case in any of the four listings.

Medical Industry Pairings

Only one medical entity had a FIRST member SOC in place. That was the Ohio State University Medical Center. Given that it was virtually impossible to know the number of records contained in each medical organization a decision made to direct the search by finding an organization within the same state and operating in a city with smaller population than that of Columbus where Ohio State University is based. Of course the type of breach was kept identical in all of the cases.

Government Sector Pairings

In order to control for the number of records in the government sector the strategy that was chosen was to follow the United States governmental organizational structure. The hierarchy of US government starts with the nationwide government on the top and continues to states, counties and cities. Therefore matches were drawn from organizations that belong to the same or lower hierarchical level.

Finance Industry Pairings

When it comes to the finance industry most of the firms that have a FIRST approved embedded SOC are financial behemoths in the likes of Citigroup, Bank of America, Wells Fargo and the Royal Bank of Scotland. Common logic dictates that in those cases, it would be extremely hard to have an erroneous matching by wrongfully selecting an organization of bigger size.

Having that in mind the focus shifted in finding breaches that occurred in direct competitors of those organizations. Since all of the organizations in this category are publicly traded, direct competitors were defined as those listed as such in the webpages of Yahoo Finance, the New York and NASDAQ stock exchanges.

If appropriate listings could not be found in the previous manner, smaller organizations from the same or competing industries were selected and the focus shifted to finding breaches as similar as possible to that of the SOC listing at hand by going through the listings' storylines. If a matching couple could still not be found the original listing containing a SOC was dropped from the comparison dataset.

Retail and Other Industries Pairings

For all the other industries in the sample, the strategy of comparing direct competitors was followed. Again when such an organization could not be found reasonably smaller organizations from the same industry were selected or the listing was not paired and excluded from the comparison.

Statistical Test I – Matched Pairs Dependent Samples T-test

Once the matched samples were completed it was possible to move on with the actual statistical testing. Firstly, an inquisitive data exploration was performed to define which statistical testing method was fit to use with the data at hand. Before moving on Table 5.5 sums up the test's hypotheses.

Hypothesis	Description
H_0	Organizations that have a well-established SOC suffer from data breaches that result in an equal or significantly higher number of records improperly accessed compared to organizations that don't have such a SOC in place.
H_1	Organizations that have a well-established SOC suffer from data breaches that result in a significantly lower number of records improperly accessed compared to similar or smaller organizations that don't have such a SOC in place.

Table 5.5: SOC Threat Control Test Hypotheses Table

Data Exploration and Descriptive Statistics

As is mandated by proper statistical analysis methods before proceeding with any statistical test an inquisitive exploration of the dataset that was formed was conducted. Figures 5.11 and 5.12 provide an overview of the main descriptive statistics of the two groups concerning the total records breached variable. All of the descriptive statistics are presented in pairs of similar content with the non SOC group coming first.

Statistics

Total Records Breached - Paired Non SOC Breaches

N	Valid	25
	Missing	0
Mean		2736037,72
Std. Deviation		8549599,847
Skewness		3,939
Std. Error of Skewness		,464
Kurtosis		16,329
Std. Error of Kurtosis		,902

Figure 5.11: Non SOC Group Statistics

Statistics

Total Records Breached - SOC Involvement

N	Valid	25
	Missing	0
Mean		474122,96
Std. Deviation		1696071,537
Skewness		4,784
Std. Error of Skewness		,464
Kurtosis		23,429
Std. Error of Kurtosis		,902

Figure 5.12: SOC Group Statistics

The initial data observation shows that the SOC group has a lower mean value (μ_{SOC}= 474.123) than the non-SOC ($\mu_{Non\text{-}SOC}$= 2.736.038). However, we also see that the data are heavily positively skewed (sk_{SOC}=4,784, $sk_{Non\text{-}SOC}$= 3,939) on both samples. Moreover, both of the samples appear to be leptokurtic in nature (ku_{SOC}=23,429, $ku_{Non\text{-}SOC}$=16,329).

Those final two observations lead us to believe that none of the samples follow the Gaussian distribution. Therefore the Kolmogorov-Smirnov and Shapiro-Wilk tests have been employed to test for normality. The results are shown in Figure 5.13.

Tests of Normality

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Total Records Breached - SOC Involvement	,390	25	,000	,300	25	,000
Total Records Breached - Paired Non SOC Breaches	,442	25	,000	,367	25	,000

a. Lilliefors Significance Correction

Figure 5.13: Tests of Normality for the Records Breached Variable in the SOC and Non-SOC Groups

All of the normality tests are highly significant in both of the groups indicating that the normal distribution is not followed by the samples. This means that parametric tests cannot be used to test differences between the samples. To graphically confirm this finding, histograms of the two groups were drawn. They are introduced in Figures 5.14 and 5.15. Take note that for ease of reading the Z transformation has been applied to the total breached records variable.

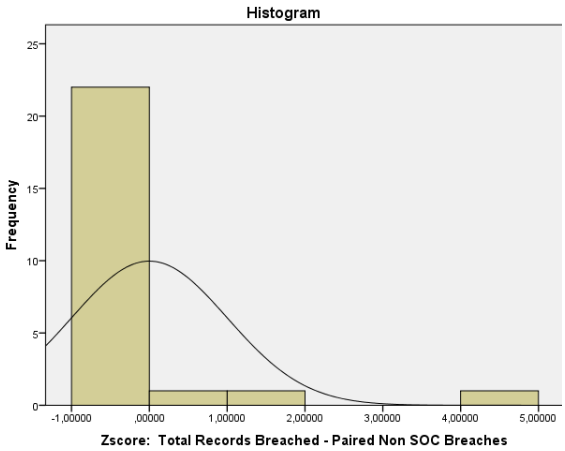


Figure 5.14: Histogram of Records Breached on Non-SOC Group (Z-Scores)

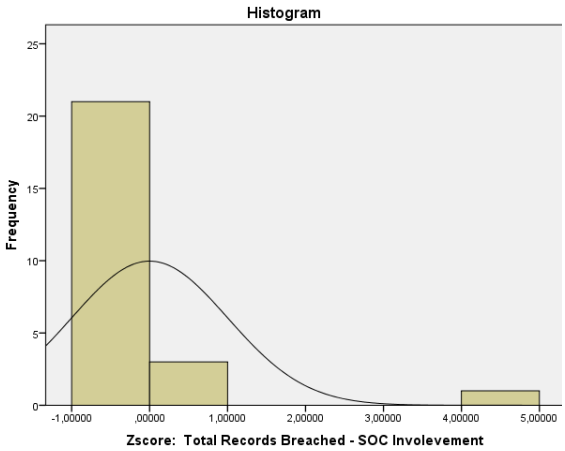


Figure 5.15: Histogram of Records Breached on SOC Group (Z-Scores)

By observing the distributions the hypothesis that the data follow the log-normal distribution instead of the Gaussian one was made. QQ plots and normality tests were employed to test that hypothesis. The QQ plots drawn are shown in Figures 5.16 and 5.17 for non SOC and SOC breaches respectively.

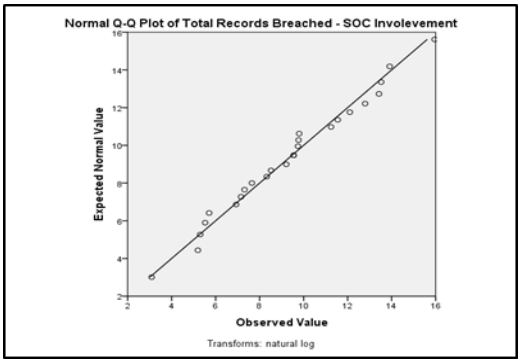


Figure 5.16: QQ Plot of Log Transformation for SOC Group

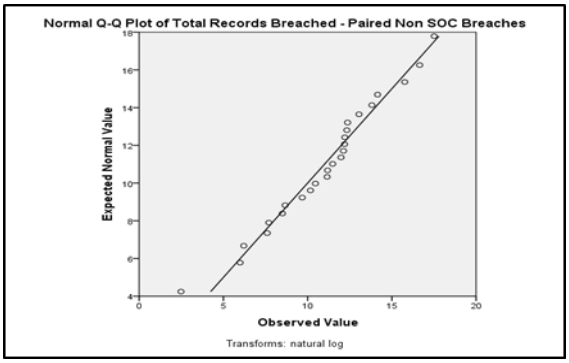


Figure 5.17: QQ Plot of Log Transformation for Non-SOC Group

The hypothesis of log-normality seemed to be confirmed by the QQ plots therefore normality tests were employed on a new variable which equaled the natural logarithm value of the total records breached one. The equation used is shown below:

$$Natural\ Log\ of\ Records = \ln(Total\ Records\ Breached)$$

Figure 5.18 shows the results of the normality tests. The tests clearly show that the newly computed variables follow the normal distribution. This, combined with the fact, that the natural logarithm is a genuinely monotonically increasing (therefore order preserving) function allows us to test our hypothesis through the natural logarithm variables and with using statistically stronger parametric tests.

Tests of Normality

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Natural Logarithm of Records Breached - SOC Involvement	,120	25	,200*	,982	25	,914
Natural Logarithm of Records Breached - Non SOC Paired Breaches	,116	25	,200*	,976	25	,793

*. This is a lower bound of the true significance.

a. Lilliefors Significance Correction

Figure 5.18: Normality Tests of Total Records Breached Log-Normal Transformation

Test Results

Keeping in mind the fact above, a one tailed, matched pair, samples t-test was chosen to test our hypothesis with a significance level (Sig) of .05. The results of the test are shown in Figures 5.19 and 5.20.

Paired Samples Statistics

		Mean	N	Std. Deviation	Std. Error Mean
Pair 1	Natural Logarithm of Records Breached - SOC Involvement	9,312828	25	3,2095808	,6419162
	Natural Logarithm of Records Breached - Non SOC Paired Breaches	11,017068	25	3,4484354	,6896871

Figure 5.19: Paired Samples Test Group Descriptive Statistics

Paired Samples Test

		Paired Differences					t	df	Sig. (2-tailed)
		Mean	Std. Deviation	Std. Error Mean	95% Confidence Interval of the Difference Lower	Upper			
Pair 1	Natural Logarithm of Records Breached - SOC Involvement - Natural Logarithm of Records Breached - Non SOC Paired Breaches	-1,7042400	3,0603998	,6120800	-2,9675110	-,4409690	-2,784	24	,010

Figure 5.20: Paired Samples Test Outcome

On average organizations with a FIRST member SOC in place experienced data breaches of lesser magnitude in terms of the amount of records breached. The difference was significant with $t(24)=-2.784$,$p=0.010 < 0.05$. Moreover, the effect size was $r= 0.494$ and was therefore characterized as medium according to the widely accepted standards set by Cohen (1992).

Nonetheless, the fact that the natural logarithm transformation was used means that interpretation of the results can be only made in terms of increasing scores (Osborne, 2002). Thus, in order to draw conclusions based directly on the number of records breached a non-parametric test was used. The test and the procedure followed are introduced in the next section.

Statistical Test II – Wilcoxon Signed-Rank Test

The dataset used for the non-parametric procedure was exactly the same as for the parametric one apart from one difference. Given the significant results of the previous test all of the randomly selected matches were substituted with the non-SOC listing that yielded the lowest amount of records breached. In this manner, any doubt that the previous results were somehow influenced by the random selection process could be lifted in case the result remained significant.

Having the above in mind a one tailed, Wilcoxon signed-rank test was chosen with significance level of 0.05. The hypotheses are identical to those of the previous test and are summarized in Table 5.6.

Hypothesis	Description
H_0	Organizations that have a well-established SOC suffer from data breaches that result in an equal or significantly higher number of records improperly accessed compared to organizations that don't have such a SOC in place.
H_1	Organizations that have a well-established SOC suffer from data breaches that result in a significantly lower number of records improperly accessed compared to similar or smaller organizations that don't have such a SOC in place.

Table 5.6: Wilcoxon Signed Ranks Test Hypothesis

The descriptive statistics concerning the test as well as its results of are shown in Figure 5.21 and Figure 5.22.

Ranks

		N	Mean Rank	Sum of Ranks
Total Records Breached - SOC Involvement - Paired Breach Total Records	Negative Ranks	19[a]	13,89	264,00
	Positive Ranks	6[b]	10,17	61,00
	Ties	0[c]		
	Total	25		

a. Total Records Breached - SOC Involvement < Paired Breach Total Records

b. Total Records Breached - SOC Involvement > Paired Breach Total Records

c. Total Records Breached - SOC Involvement = Paired Breach Total Records

Figure 5.21: Wilcoxon Signed Rank Test Rank Statistics

The test shows clearly that the amount of personally identifiable records breached for the SOC group (Mdn_{SOC}=14000) is significantly lower than for the non SOC group (Mdn_{NonSOC}=700000), T=0, p<.05, r=-.54.

Test Statistics[a]

	Total Records Breached - SOC Involvement - Paired Breach Total Records
Z	-2,731[b]
Asymp. Sig. (2-tailed)	,006

a. Wilcoxon Signed Ranks Test

b. Based on positive ranks.

Figure 5.22: Wilcoxon Signed Rank Test Result

Having both of the tests to agree in their findings led us to perform a final statistical test to observe whether there were any industries in the sample that should consider a SOC implementation an information security priority based on the types of breaches their industry has suffered from. The test is described in the following Chapter.

Chapter Conclusion

In this chapter both a parametric as well as a non-parametric were used to test whether SOCs indeed provide better organizational performance in terms of threat control. This performance was tested by forming matched pairs of organizations with and without a well-established SOC that had suffered data breaches over the past ten years. Both of the tests concur that the number of personally identifiable records breached among the SOC group were significantly less than on the non-SOC group.

This finding strongly indicates that SOCs outperform conventional information security approaches when it comes to threat control. Although it could not be directly derived from our testing, assuming that SOCs outperform conventional approaches when it comes to threat prevention also is not a big mental leap to make. Given that threat control and prevention is the capability that most information security business benefits derive from, this builds a very strong case for SOCs.

Another insight that can be drawn from the tests concerns the rationalization of investing in a SOC. The median difference of records breached among the SOC and Non-SOC groups amounted to 56000 records. Ponemon Institute (2014) has found that on average one breached record cost to $201. If we multiply those two numbers we can see that an organization can avoid costs of more than 11.25 million dollars.

The most conservative academic approach relating to IT investments in information security has been devised by Gordon and Loeb (2002). They theorized that a firm should spend no more than 37% of their expected losses due to a data breach on information security investments. If we multiply that percentage with the amount calculated above we see that the minimum break-even point for a SOC investment is a bit more than 4.1 million dollars.

Chapter 6 – Data Breach Comparison of Impact Testing

The previous chapter has shown that SOCs indeed provide organizations with enhanced information security performance. They therefore set a strong foundation for firms to realize a variety of business benefits.

Nonetheless, SOCs cannot protect organizations from all data breach types. We therefore sought to examine whether there is a significant difference in the amount of records improperly accessed due to breach types a SOC can protect against and not.

Moreover, it was deemed wise to perform the aforementioned comparison on a per industry basis. In that manner, executive decision makers can have an additional source of information when contemplating the possibility of a SOC investment.

This chapter described the steps used in order to tackle this thesis' second research question. As a reminder to the reader this was:

RQ 3: *Which industries among the financial, insurance, medical, nonprofit, government and retail ones are significantly differently impacted by data breach types relating to SOCs compared to data breaches unrelated to SOCs??*

To answer this question an independent samples testing approach was employed. For each of the industries mentioned within our research question the amount of records breached by SOC relevant data breach types was compared to breach types a SOC is not purposed to protect against or respond to.

The dataset that was used for the tests was the initial dataset of all listings with known numbers of records breached except for the listings where the breach cause was unknown. The resulting dataset consisted of 2177 listings. All of the data breach listings were classified according to their type as SOC or non SOC relevant. Moreover a division according to the industry that the inflicted organizations belonged to was made. Thus six sub-datasets were conjured.

The division of the listings according to industry and SOC relevancy is shown in Figure 6.1. The same division but accounting for the total number of records breached instead of the number of listings is shown in Figure 6.2. Each of the industry datasets as well as the subgroups within them differed in terms of statistical distributions when it came to the records breached variable. Therefore by also having the insights from the previously conducted tests in mind the process depicted in Figure 6.3 was followed to determine the proper statistical to test to be executed.

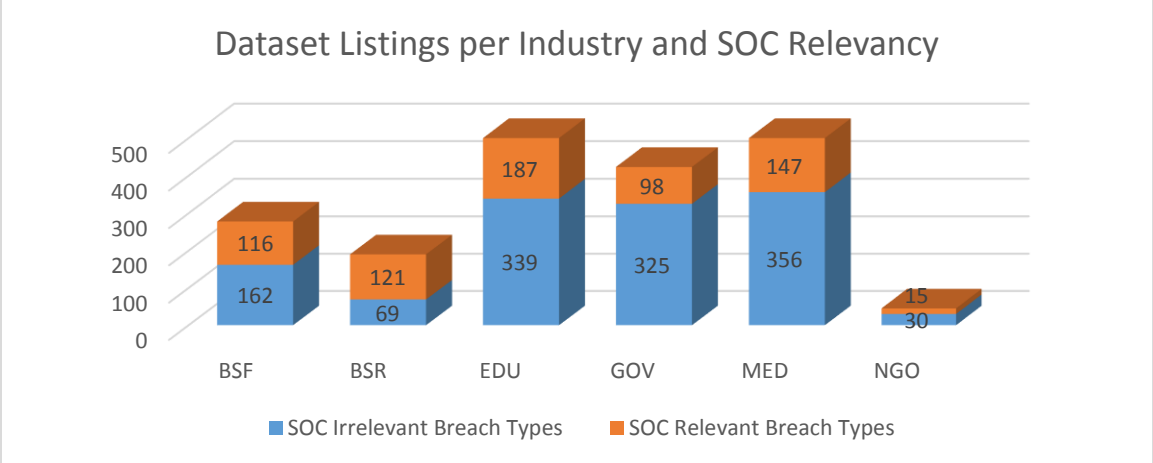


Figure 6.1: Division of Industry Prioritization Testing Dataset's Listings per Industry and SOC Relevancy

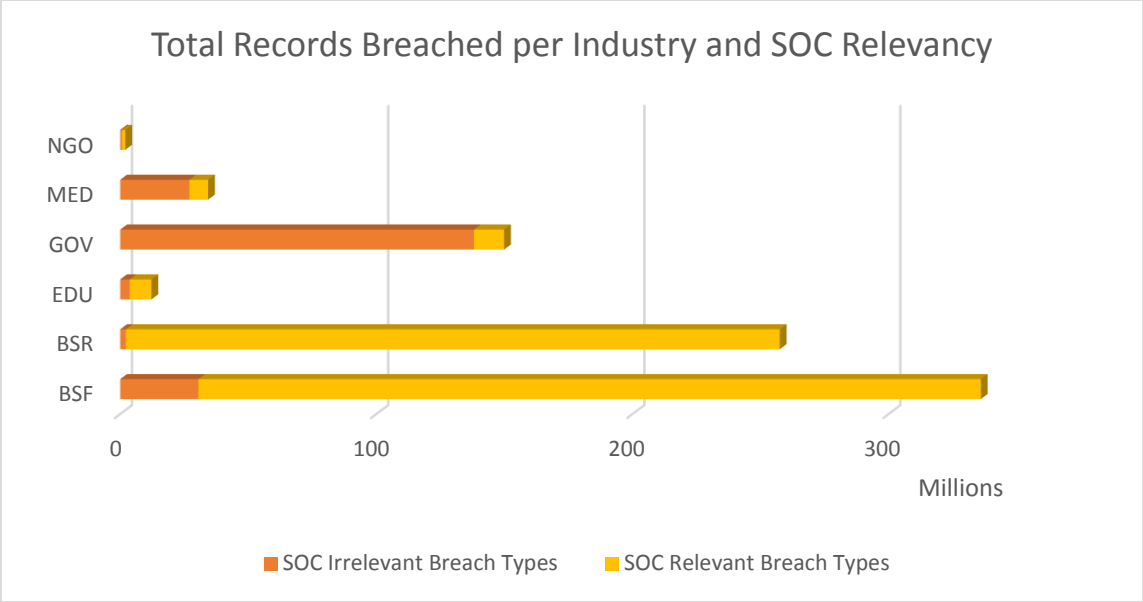


Figure 6.2: Total Records Breached per Industry and SOC Relevancy

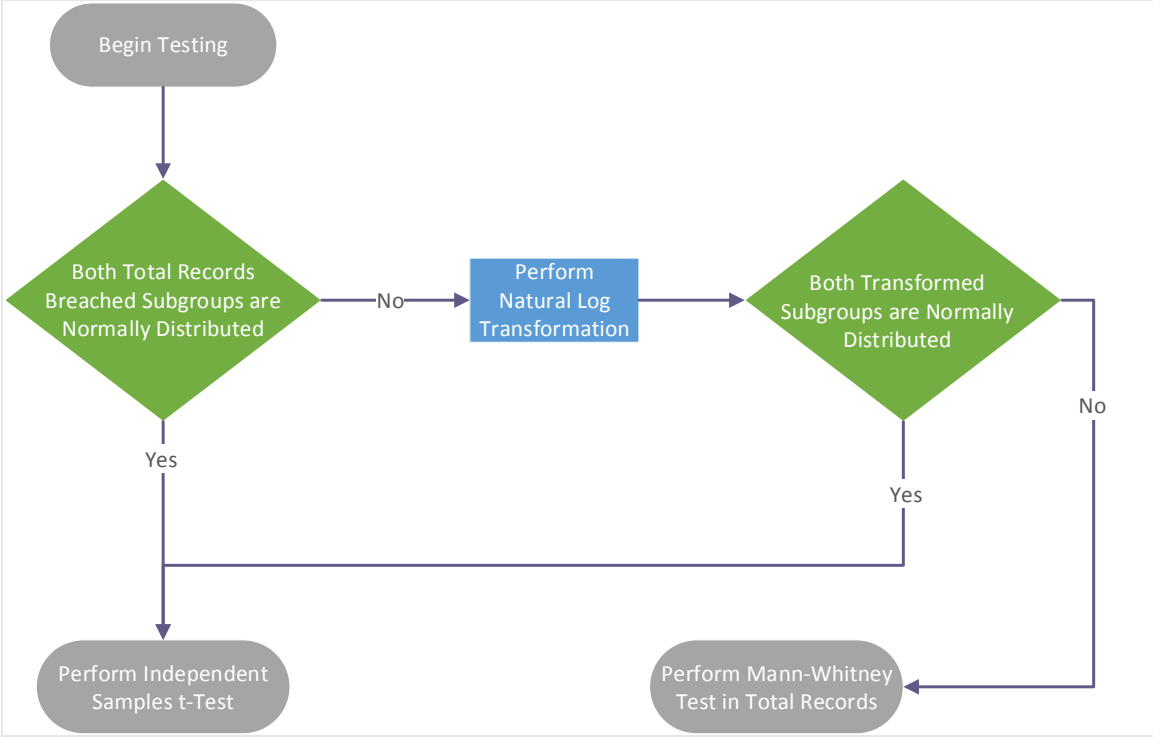


Figure 6.3: Statistical Test Selection Process

Following the statistical analysis as well as the results of the relevant test for each industry are presented.

Financial and Insurance Industry

Abiding to our test selection process the normality of the total records breached variable for the SOC relevant and irrelevant, breach type, subgroups was tested. The results were negative thus the natural logarithm transformation was used. Nonetheless, the SOC relevant breaches subgroup still remained unnaturally distributed. Figures 6.4 and 6.5 summarize the normality test results.

Tests of Normality[a]

	Kolmogorov-Smirnov[b]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Total Records Breached	,431	162	,000	,160	162	,000
Natural Log of Total Records Breached	,056	162	,200*	,985	162	,078

*. This is a lower bound of the true significance.

a. SOC Relevant Breach = SOC Irrelevant Breach Type

b. Lilliefors Significance Correction

Figure 6.4: Normality Tests for the SOC Irrelevant Breaches Subgroup in the Financial Industry Dataset

Tests of Normality[a]

	Kolmogorov-Smirnov[b]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Total Records Breached	,462	116	,000	,177	116	,000
Natural Log of Total Records Breached	,113	116	,001	,942	116	,000

a. SOC Relevant Breach = SOC Relevant Breach Type

b. Lilliefors Significance Correction

Figure 6.5: Normality Tests for the SOC Relevant Breaches Subgroup in the Financial Industry Dataset

Therefore according to the test plan a two-tailed, Mann-Whitney test was used to test whether a significant difference in the amount of records breached occurred between SOC relevant and irrelevant breach types. The hypotheses of the test are summarized in Table 6.1 while the results of the ensuing test are summarized in Figures 6.6 and 6.7.

Hypothesis	**Description**
H0	In the finance and insurance industry, SOC relevant data breach types result in amounts of records breached significantly not different from SOC irrelevant data breach types.
H1	In the finance and insurance industry, SOC relevant data breach types result in amounts of records breached significantly different from SOC irrelevant data breach types.

Table 6.1: Finance and Insurance Industry Test Hypotheses

Ranks

	SOC Relevant Breach	N	Mean Rank	Sum of Ranks
Total Records Breached	SOC Irrelevant Breach Type	162	143,54	23253,00
	SOC Relevant Breach Type	116	133,86	15528,00
	Total	278		

Figure 6.6: Mann-Whitney Test Rank Statistics – Finance and Insurance Industry

Test Statistics[a]

	Total Records Breached
Mann-Whitney U	8742,000
Wilcoxon W	15528,000
Z	-,989
Asymp. Sig. (2-tailed)	,322
Exact Sig. (2-tailed)	,323
Exact Sig. (1-tailed)	,162
Point Probability	,000

a. Grouping Variable: SOC Relevant Breach

The results show that within the finance and insurance industry the amount of records breached by SOC relevant breach types (*Mdn*=1000) did not differ significantly from SOC irrelevant breach types (*Mdn*=2970) U=8742, z=-.989, ns, r=-.05.

Figure 6.7: Mann-Whitney Test Results – Finance and Insurance Industry

Retail and Merchant Industry

Again the normality of the total records breached variable for the SOC relevant and irrelevant, breach type subgroups was tested. The results were negative thus the natural logarithm transformation was used. Nonetheless, the SOC relevant breaches subgroup still remained unnaturally distributed. Figures 6.8 and 6.9 summarize the normality test results.

Tests of Normality[a]

	Kolmogorov-Smirnov[b]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Total Records Breached	,381	69	,000	,325	69	,000
Natural Logarithm of Total Records Breached	,081	69	,200*	,969	69	,081

*. This is a lower bound of the true significance.

a. SOC Relevant Breach = SOC Irrelevant Breach Type

b. Lilliefors Significance Correction

Figure 6.8: Normality Tests for the SOC Irrelevant Breaches Subgroup in the Retail and Merchant Industry Dataset

Tests of Normality[a]

	Kolmogorov-Smirnov[b]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Total Records Breached	,469	121	,000	,186	121	,000
Natural Logarithm of Total Records Breached	,148	121	,000	,902	121	,000

a. SOC Relevant Breach = SOC Relevant Breach Type

b. Lilliefors Significance Correction

Figure 6.9: Normality Tests for the SOC Relevant Breaches Subgroup in the Retail and Merchant Industry Dataset

Once more, a two-tailed, Mann-Whitney test was used to test whether a significant difference in the amount of records breached occurred between SOC relevant and irrelevant breach types. The hypotheses of the test are summarized in Table 6.2.

Hypothesis	Description
H_0	In the retail and merchant industry, SOC relevant data breach types result in amounts of records breached significantly not different from SOC irrelevant data breach types.
H_1	In the retail and merchant industry, SOC relevant data breach types result in amounts of records breached significantly different from SOC irrelevant data breach types.

Table 6.2: Retail and Merchnt Industry Test Hypotheses

The results of the test are summarized in Figures 6.10 and 6.11.

Ranks

	SOC Relevant Breach	N	Mean Rank	Sum of Ranks
Total Records Breached	SOC Irrelevant Breach Type	69	101,09	6975,50
	SOC Relevant Breach Type	121	92,31	11169,50
	Total	190		

Figure 6.10: Mann-Whitney Test Rank Statistics – Retail and Merchant Industry

Test Statistics[a]

	Total Records Breached
Mann-Whitney U	3788,500
Wilcoxon W	11169,500
Z	-1,059
Asymp. Sig. (2-tailed)	,290

a. Grouping Variable: SOC Relevant Breach

The results show that within the finance and insurance industry the amount of records breached by SOC relevant breach types (*Mdn*=400) did not differ significantly from SOC irrelevant breach types (*Mdn*=1200) U=3788.5, z=-1.059, ns, r=0.07.

Figure 6.11: Mann-Whitney Test Results – Retail and Merchant Industry

Education Industry

Once more the normality tests for the total breached records variable showed non-normality of the data. Therefore, the natural logarithm transformation was used. This time however, the Kolmogorov Smirnov test showed that the natural logarithm transformation proved to be effective in both subgroups. The Shapiro-Wilk test did indeed prove to be significant but given the sample sizes ($N_{SOC\text{-}Relevant}$=187, $N_{SOC\text{-}Irrelevant}$=339) this finding was ignored. This is because the Shapiro-Wilk test is less effective than the KS test in big sample sizes (Field, 2013). Figures 6.12 and 6.13 summarize the normality test results.

Tests of Normality[a]

	Kolmogorov-Smirnov[b]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Total Records Breached	,366	339	,000	,344	339	,000
Natural Logarithm of Total Records Breached	,048	339	,061	,990	339	,026

a. SOC Relevant Breach = SOC Irrelevant Data Breach Type

b. Lilliefors Significance Correction

Figure 6.12: Normality Tests for the SOC Irrelevant Breaches Subgroup in the Education Industry Dataset

Tests of Normality[a]

	Kolmogorov-Smirnov[b]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Total Records Breached	,334	187	,000	,437	187	,000
Natural Logarithm of Total Records Breached	,055	187	,200*	,973	187	,001

*. This is a lower bound of the true significance.

a. SOC Relevant Breach = SOC Relevant Data Breach Type

b. Lilliefors Significance Correction

Figure 6.13: Normality Tests for the SOC Relevant Breaches Subgroup in the Education Industry Dataset

Given the normality test results an independent samples a two tailed t-test was conducted. The hypotheses of the test are shown in Table 6.3.

Hypothesis	**Description**
H_0	In the education industry, SOC relevant data breach types result in amounts of records breached significantly not different from SOC irrelevant data breach types.
H_1	In the education industry, SOC relevant data breach types result in amounts of records breached significantly different from SOC irrelevant data breach types.

Table 6.3: Education Industry Test Hypotheses

The t-test's results are shown in Figures 6.14 and 6.15.

Group Statistics

	SOC Relevant Breach	N	Mean	Std. Deviation	Std. Error Mean
Natural Logarithm of Total Records Breached	SOC Irrelevant Data Breach Type	339	7,3044	2,19077	,11899
	SOC Relevant Data Breach Type	187	8,9592	2,26219	,16543

Figure 6.14: Independent Samples T-Test Group Statistics – Education Industry

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means						
									95% Confidence Interval of the Difference	
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Lower	Upper
Natural Logarithm of Total Records Breached	Equal variances assumed	,003	,953	-8,196	524	,000	-1,65477	,20189	-2,05139	-1,25816
	Equal variances not assumed			-8,121	373,257	,000	-1,65477	,20377	-2,05546	-1,25408

Figure 6.15: Independent Samples T-Test Results – Education Industry

The results show that within the education industry the average amount of records breached by SOC relevant breach types differs significantly from SOC irrelevant breach types $t(524)=-8.196$,$p=.000 < 0,05$, $r=0.337$. In fact, the test shows that on average SOC relevant data breaches result in a higher amount of records improperly accessed than SOC irrelevant ones.

Government Industry

With the government industry dataset a Mann-Whitney test had to be employed since the SOC relevant breaches subgroup did not fulfill the normality criterion. Figures 6.16 and 6.17 show the normality test results. The test's hypotheses are shown in Table 6.4 while its results are shown in Figures 6.18 and 6.19.

Tests of Normality[a]

	Kolmogorov-Smirnov[b]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Total Records Breached	,428	98	,000	,160	98	,000
Natural Logarithm of Total Records Breached	,072	98	,200*	,984	98	,289

*. This is a lower bound of the true significance.

a. SOC Relevant Breach = SOC Irrelevant Breach Type

b. Lilliefors Significance Correction

Figure 6.16: Normality Tests for the SOC Irrelevant Breaches Subgroup in the Government Industry Dataset

Tests of Normality[a]

	Kolmogorov-Smirnov[b]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Total Records Breached	,462	325	,000	,066	325	,000
Natural Logarithm of Total Records Breached	,059	325	,008	,985	325	,002

a. SOC Relevant Breach = SOC Relevant Breach Type

b. Lilliefors Significance Correction

Figure 6.17: Normality Tests for the SOC Relevant Breaches Subgroup in the Government Industry Dataset

Hypothesis	**Description**
H_0	In the government industry, SOC relevant data breach types result in amounts of records breached significantly not different from SOC irrelevant data breach types.
H_1	In the government industry, SOC relevant data breach types result in amounts of records breached significantly different from SOC irrelevant data breach types.

Table 6.4: Government Industry Test Hypotheses

Ranks

	SOC Relevant Breach	N	Mean Rank	Sum of Ranks
Total Records Breached	SOC Relevant Breach Type	325	207,57	67459,00
	SOC Irrelevant Breach Type	98	226,70	22217,00
	Total	423		

Figure 6.18: Mann-Whitney Test Rank Statistics – Government Industry

Test Statistics[a]

	Total Records Breached
Mann-Whitney U	14484,000
Wilcoxon W	67459,000
Z	-1,358
Asymp. Sig. (2-tailed)	,174

a. Grouping Variable: SOC Relevant Breach

The results show that within the government industry the amount of records breached by SOC relevant breach types (*Mdn*=2359) did not differ significantly from SOC irrelevant breach types (*Mdn*=5700) U=14484, z=-1.358, ns, r=0.279.

Figure 6.19: Mann- Whitney Test Results – Government Industry

Medical Industry

As with the government industry a Mann-Whitney test had to be employed for the medical industry also since the SOC relevant breaches subgroup did not fulfill the normality criterion. Figures 6.20 and 6.21 show the results of the normality for the two groups. Figures 6.22 and 6.23 show the results of the following Mann-Whitney test while Table 6.5 presents its hypotheses.

Tests of Normality[a]

	Kolmogorov-Smirnov[b]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Total Records Breached	,428	98	,000	,160	98	,000
Natural Logarithm of Total Records Breached	,072	98	,200*	,984	98	,289

*. This is a lower bound of the true significance.

a. SOC Relevant Breach = SOC Irrelevant Breach Type

b. Lilliefors Significance Correction

Figure 6.20: Normality Tests for the SOC Irrelevant Breaches Subgroup in the Medical Industry Dataset

Tests of Normality[a]

	Kolmogorov-Smirnov[b]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Total Records Breached	,462	325	,000	,066	325	,000
Natural Logarithm of Total Records Breached	,059	325	,008	,985	325	,002

a. SOC Relevant Breach = SOC Relevant Breach Type

b. Lilliefors Significance Correction

Figure 6.21: Normality Tests for the SOC Relevant Breaches Subgroup in the Medical Industry Dataset

Hypothesis	**Description**
H_0	In the medical industry, SOC relevant data breach types result in amounts of records breached significantly not different from SOC irrelevant data breach types.
H_1	In the medical industry, SOC relevant data breach types result in amounts of records breached significantly different from SOC irrelevant data breach types.

Table 6.5: Medical Industry Test Hypotheses

Ranks

	SOC Relevant Breach	N	Mean Rank	Sum of Ranks
Total Records Breached	SOC Irrelevant Data Breach Type	356	273,47	97356,50
	SOC Relevant Data Breach Type	147	200,00	29399,50
	Total	503		

Figure 6.22: Mann-Whitney Test Rank Statistics – Medical Industry

Test Statistics[a]

	Total Records Breached
Mann-Whitney U	18521,500
Wilcoxon W	29399,500
Z	-5,156
Asymp. Sig. (2-tailed)	,000

a. Grouping Variable: SOC

Figure 6.23: Mann-Whitney Test Results – Medical Industry

The test shows clearly that within the medical industry, the amount of records breached by SOC irrelevant data breach types (*Mdn*=4314) differs significantly from records accessed improperly by SOC relevant data breach types (*Mdn*=919), U=18521.5, p<.05, r=0.22.

In fact, the test shows that on average SOC irrelevant data breaches result in higher amounts of records being breached.

Nonprofit Organizations

The final test of this test group concerned nonprofit organizations. In this case the normality tests for the natural logarithm transformation of the records breached variable proved insignificant. Figures 6.24 and 6.25 show the normality tests' results.

Tests of Normality[a]

	Kolmogorov-Smirnov[b]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Total Records Breached	,366	30	,000	,400	30	,000
Natural Logarithm of Total Records Breached	,111	30	,200*	,968	30	,499

*. This is a lower bound of the true significance.

a. SOC Relevant Breach = SOC Irrelevant Breach

b. Lilliefors Significance Correction

Figure 6.24: Normality Tests for the SOC Irrelevant Breaches Subgroup in the Nonprofit Organizations Dataset

Tests of Normality[a]

	Kolmogorov-Smirnov[b]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Total Records Breached	,411	15	,000	,362	15	,000
Natural Logarithm of Total Records Breached	,213	15	,066	,931	15	,282

a. SOC Relevant Breach = SOC Relevant Breach

b. Lilliefors Significance Correction

Figure 6.25: Normality Tests for the SOC Relevant Breaches Subgroup in the Nonprofit Organizations Dataset

The hypotheses of the subsequent independent samples t-test are shown in Table 6.6 while its results in Figures 6.26 and 6.27.

Hypothesis	Description
H_0	Among nonprofit organizations, SOC relevant data breach types result in amounts of records breached significantly not different from SOC irrelevant data breach types.
H_1	Among nonprofit organizations, SOC relevant data breach types result in amounts of records breached significantly different from SOC irrelevant data breach types.

Table 6.6: Nonprofit Organizations Test Hypotheses

Group Statistics

	SOC Relevant Breach	N	Mean	Std. Deviation	Std. Error Mean
Natural Logarithm of Total Records Breached	SOC Irrelevant Breach	30	7,2078	2,70423	,49372
	SOC Relevant Breach	15	7,7815	3,45460	,89197

Figure 6.26: Independent Samples T-Test Group Statistics – Nonprofit Organizations

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means						
									95% Confidence Interval of the Difference	
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Lower	Upper
Natural Logarithm of Total Records Breached	Equal variances assumed	2,852	,099	-,611	43	,544	-,57371	,93902	-2,46742	1,31999
	Equal variances not assumed			-,563	22,857	,579	-,57371	1,01950	-2,68344	1,53601

Figure 6.27: Independent Samples T-Test Results – Nonprofit Organizations

Among nonprofit organizations the amount of records breached by SOC relevant data breach types does not differ significantly from SOC irrelevant ones t(43)=-.611 ,ns , r=0.092.

Chapter Conclusion

In this chapter six industries have been examined in order to establish whether among the industry's members SOC relevant data breach types resulted in a significantly different amount of records breached than non SOC relevant breach types. Table 6.7 provides a summary of the datasets that have been used while the tests that have been conducted as well as their results are presented in Table 6.8.

Industry	Number of SOC Related Breaches	Total Records Breached by SOC Related Breaches	Number of Non-SOC Related Breaches	Total Records Breached by Non-SOC Related Breaches
Financial and Insurance	116	305,870,296	162	30,538,415
Retail and Merchant	121	255,264,654	69	2,232.216
Education	187	8,502,168	339	3,719,152
Government	98	11,740,161	325	138,156,053
Medical	147	7,321,657	356	27,000,376
Nonprofit	15	1,254,021	30	734,245

Table 6.7: Industry Datasets Summary

Industry	Test Employed	Target Variable	Significance	Effect Size
Financial and Insurance	Mann-Whitney Test	Records Breached	Not Significant	0.5
Retail and Merchant	Mann-Whitney Test	Records Breached	Not Significant	0.07
Education	T-Test	Ln of Records Breached	.000	0.337
Government	Mann-Whitney Test	Records Breached	Not Significant	0.279
Medical	Mann-Whitney Test	Records Breached	.000	0.22
Nonprofit	T-Test	Ln of Records Breaches	Not Significant	0.092

Table 6.8: Industry Testing Result Summary

In four out of the six cases the results of the tests were not significant. This suggests that both SOC related and unrelated breaches have similar impact to organizations in terms of records breached. Therefore organizations participating in those industries could move towards risk reduction by examining the frequency of the different data breach types. Moreover, it is important for those industries to approach information security in a holistic manner that would enable them to show resiliency against the whole spectrum of data breach types.

The tests produced two significant results also. Those concerned the education and medical industries. Despite the fact that our hypothesis was formed for a two tailed test it was easy to deduct from the results that when it comes to the education industry a SOC investment could be prioritized in the minds of decision makers over other information security measures. This is derived from the fact that SOC relevant breach types caused a significantly larger impact to this industry in terms of records breached.

On the contrary when it comes to the medical industry it was SOC irrelevant data breaches that produced a larger amount of records breached. Therefore if a business case is to be built for SOCs in this industry it cannot be based only on the advanced threat control and protection capabilities of a SOC. It should extend to other issues like regulatory compliance and the support a SOC can provide when it comes to it. Lastly, members of the medical industry should prioritize their abilities to respond to and protect against the theft of portable and static devices, the loss of physical records and their accidental disclosure.

Chapter 7 – Conclusion

In this chapter a discussion is presented concerning the research findings and conclusions of this thesis. Initially the outcome of each defined research question is going to be discussed. Continuing the limitations of this research are presented. Finally, some propositions for future research are made based on the outcome and experiences drawn from this research.

Research Questions' Outcomes

First Research Question

RQ 1: *How can Security Operations Centers be viewed from a business decision maker's perspective?*
SQ 1.1: *What is a high level description of a SOC concerning its goals, functions and operating aspects?*
SQ 1.2: *What is the state of the art when it comes to information security? What are the field's shaping forces and the main threats and threat actors towards organizations?*
SQ 1.3: *What are the business drivers underlying a SOC implementation and the enhanced information security performance it could provide?*

The first thing that needs to be understood by any decision maker concerning SOCs is that they differ widely in nature than traditional information security solutions. SOCs, although being heavily underpinned by technology, are not a technological solution aimed to provide protection against a particular type of cyber threat. They are organizational structures, consisting of a technology, people and process aspect that aim to orchestrate and leverage the information security technologies an organization is in possession of in order to deliver a holistically enhanced information security posture.

To put it another way a question in the likes of which is a better a SOC is not a really valid one since SOCs can and will vary between them in terms of utilized security solutions, organizational structure and services offered. Nonetheless, all SOCs share the same high level goals which in their own turn are based on the capabilities offered by common functional domains.

Those goals are situational awareness deliverance, risk and downtime reduction, threat control and prevention, diminishing of administrative overhead, forensics as well as audit and compliance support. The functional domains through which those goals are achieved are log collection, analysis and retention, threat identification and reaction, event correlation, incident management, reporting and security environment monitoring.

SOCs are indeed inherently complex but their complexity is mandated both by the variety of threats they have to face as well as the environment in which they operate. An array of threat actor groups exist most of which have significant technical skills that enable them to utilize the even wider range of attack methods that are in place. Even if their technical capabilities are limited, an organized cyber market exists where those skills can be hired at will.

This market is indicative of the evolution of the information security environment in which most of threat actors are operating with the goal of financial profit. Not only are those actors highly active but they are also able to perform their actions in relative freedom since most of cybercrimes remain unpunished.

Additionally, when it comes to information security the technological balance of power is currently in the hands of attacking parties. The defending side has to protect every single system in order to achieve its goal while the attacking one needs to find only one sole point of entry. Those points of entry are usually system vulnerabilities.

Concerning vulnerabilities it is vital to note that they are ever-present within the information security environment. This is directly derived from the manner in which the software industry operates and therefore is not expected to change.

What makes things even more convoluted within the current information security landscape is the fact that the cyber insurance market is still underdeveloped and therefore can't be employed as a safety net by organizations that suffer from information security breaches. Thus, organizations need to be proactive when it comes to protecting themselves from such breaches.

Moreover, the costs of information security failures are proving very hard to quantify with great variations between estimations. Nonetheless, even the modest among them reach to conclusions involving monetary sums significant to every organization.

The information security environment indeed proves to be a hostile one. SOC functions and capabilities however form a straightforward match to the requirements that the aforementioned environment poses. Thus there are significant business benefits to be derived from a SOC implementation which need to be considered by a decision maker.

Those business benefits are both hard and soft. Firstly, it has been scientifically proven that the stock value of a publicly traded firm faces an extraordinary drop after the public announcement of an information security incident. What's more the current regulatory environment, especially in the European Union, makes it difficult for organizations to avoid actually announcing the breach and dealing with it internally.

Additionally, several other costs stemming from data breaches have been identified. Those are loss of business due to systems' downtime, system remediation costs, theft of intellectual property, loss of consumer and business partner trust, regulatory fines as well as legal expenses due to judicial action initiated by the aforementioned parties.

Moreover, a SOC can help an organization optimize its information security spending since it can deliver the hard data needed for proper risk analysis techniques to be used. It can also add to a firm's brand strength and reputation by both protecting it as well as serving as a basis for standardization efforts. Lastly, given all of the above a SOC can also be viewed as a contributor towards increased investor confidence.

To summarize our SOC business perspective in a single sentence: Well-managed SOCs, through an advanced combination of organizational and technological components, can assist organizations to overcome the significant adversities of the information security environment thus enabling them to reap substantial business benefits.

Second Research Question

RQ2: Does the existence of a well-established Security Operations Center lead to better organizational performance concerning information security when it comes to the hacking, card fraud, and insider data breach types?

Despite the fact that all of the theoretical arguments advocate for the viewpoint that a well-established SOC leads to better information security results to the best of the author's knowledge no scientific literature existed to support this perception.

Using a matched pair samples methodology, both a parametric as well as a non-parametric, one tailed statistical test have been conducted to establish whether data breaches that occurred to organizations with an embedded SOC resulted to fewer records being stolen than data breaches to similar organization without an embedded SOC. The results of both tests have been significant and confirmed our hypothesis that SOCs

do enable organizations to perform better when it comes to threat control. Moreover, the parametric test had an almost large effect size (0.494) while the non-parametric a purely large one (>0.5).

Given that, we can conclude that well-established SOCs indeed achieve their target of increased organizational performance when it comes to information security. This result is also of great business significance since almost all of the SOC business benefits are rooted in the SOC's ability to provide better threat control and prevention.

Third Research Question

RQ 3: Which industries among the financial, insurance, medical, nonprofit, government, and retail ones are significantly differently impacted by data breach types relating to SOCs compared to data breaches unrelated to SOCs?

Having the insights from our previous research question drawn we set forward to discover whether industries exist where SOC relevant data breach types lead to amounts of records breached significantly different to SOC irrelevant ones.

Among the industries examined only the education and medical ones had statistical tests with significant results. Among them only on the former the results leaned towards SOC investment prioritization.

Final Remarks

It is obvious that the inherently complex nature of information security in general and of SOCs in particular make it very difficult for traditional business arguments concerning SOC investments to be made. We have seen however that those arguments not only can be constructed but the current situation presses for organizations to do so.

This however underlines the need for an open dialogue between technical and non-technical executives that is not based on fear and uncertainty. Moreover, the foundation of this dialogue should be the common understanding (or perhaps admittance) that a completely secure and impenetrable system is, if not unachievable, certainly not financially sensible.

In the case of SOCs this suggests that they should not be treated as a silver bullet when it comes to information security issues. They should be considered as the foundation of business resiliency when it comes to the information security domain.

Organizations that are considering investing in a SOC should start by defining what is expected from it. Those expectations will guide the SOC's mission and should be derived by the organizations' business objectives. Moreover, the dialogue concerning them should involve higher management thus making their buy-in and support easier to obtain.

Continuing, the position of the SOC within the organizational hierarchy should be clearly defined. The SOC's position must reflect the authorities that it should have in order to complete its mission. Moreover, it is important to make clear to whom the SOC reports to. Many high level executives such as the CIO, CISO, CSO, and COO are at least partially concerned with information security and would like to be 'kept in the loop' especially during an incident. Those potential conflicts could hamper SOC operations.

This highlights the fact that a SOC's responsibilities will have it operating in areas previously belonging to multiple business domains. It is therefore important for it to be perceived as a credible partner within the enterprise. Given the inherent complexity embedded within SOC implementations and in order to achieve this credibility it would be wise for a SOC to start with a smaller set of objectives that it can confidently achieve. Moreover, all of the above indicate that the SOC should draw from the organization's pre-existing

resources and incorporate them under its organizational structure. Those resources, involving both technology and people can prove quintessential in reducing the initial budget required for a SOC implementation.

According to our analysis, a major part of this budget should be devoted to the people aspect of a SOC. We have seen that the premise of a SOC is to empower a few individuals with actionable information so that threat prevention and response are streamlined. It is therefore essential for organizations to invest in quality over quantity when it comes to the people aspect. Additionally, given the scarcity of highly qualified SOC personnel, organizations should have a development process in place in order to be able to retain those individuals.

Lastly, it is especially important for a SOC to build and leverage various external and internal partnerships. For example other SOCs could be prove to be an invaluable source of cyber threat intelligence. At the same time a SOC should develop relationships with the legal and public relationships department. The former is mandated in order for the SOC to be able to operate in a law abiding fashion especially when it comes to facing insider threats. The latter is mandated so that when a successful breach occurs brand strength will still be protected as best as possible.

It is obvious that SOC implementations are multi-faceted projects that need to take in account and manage a multitude of issues in order to be successful. However, given the hostile nature of the contemporary information security environment, they can be thought as the foundation that will give organizations the opportunity to compete within it.

To make a final and strictly personal remark, when thinking about the outcome of this thesis, the author could not but bring to memory the Boston Consulting Group fellow and professor at the Ecole Centrale in Paris, Luc de Brabandere. In his lectures about organizational learning and change, he mentions the ‘eureka’ and ‘caramba’ moments of organizational learning. They respectively refer to organizations changing their perceptions before and after the occurrence of a significant event. To this thesis’ author SOCs can be the foundation for organizations to avoid learning the hard way.

Research Limitations

There are three major limitations concerning this research. The first stems from the fact that the technological frames of reference theory that was used to formulate the skeleton of the SOC business perspective was developed to be used primarily with interviews of organizational group stakeholders as input. This is derived from the fact that its main purpose was to resolve inter-organizational, perception incongruences. In this case however literature was used as an input. This decision however, can be considered justifiable since the aim of this thesis was to build a SOC perspective concerning the business decision maker.

The second limitation concerns the fact that the dataset that was used for statistical testing consisted exclusively of data breaches that impacted organizations based in the United States. One might argue that this limits the research findings in the context of this country. Given the international nature of cybercrime though this argument can be at least partially countered. Moreover the regulatory environment of the United States made it possible for quantifiable, verified data concerning the amount of records breached to exist.

Lastly, despite the fact that SOCs perform better when their constituency’s systems have been breached the question whether SOCs perform better when it comes to preventing the breaches from happening in their first place has been at best answered asymptotically. This is attributed to the fact that, to the best to the nest of the author’s knowledge, publicly available data pertaining to attempted but unsuccessful data

breaches do not exist. It is not a long stretch however - especially given the size of organizations involved in the study – that if a SOC can provide better threat control it can also provide better threat protection.

Future Research Directions

There are three main directions future research could follow based on this thesis. Firstly, the research that has been conducted here can be extended to non US SOCs and their respective organizations. This would enable academia to examine whether SOCs provide augmented results across countries and if not what are the differences that lead to this discrepancy.

Secondly, this research can be replicated for outsourced SOC services offered by managed security providers. This would enable us to examine whether the results remain consistent when SOC functionalities are outsourced despite the misaligned incentives theory.

Lastly, the metrics for evaluating SOC performance could be extended beyond the records breached one. For example, the time it took for a breach to be identified as well as reacted upon could be two such metrics. Once those extended metrics have been established, it would be very interesting to relate better performance to the services offered by SOCs, perhaps through the use of factor analysis.

References

Aaker, D. A. (2009). *Managing Brand Equity*. New York, NY: Simon and Schuster.

Aggarwal, P., Arora, P., Neha, I., & Poonam, K. (2014). REVIEW ON CYBER CRIME AND SECURITY. *International Journal of Research in Engineering and Applied Sciences*, *02*(01), 48–51.

Ailawadi, K. L., Lehmann, D. R., & Neslin, S. A. (2003). Revenue Premium as an Outcome Measure of Brand Equity. *Journal of Marketing*, *67*(4), 1–17. doi:10.1509/jmkg.67.4.1.18688

Akamai. (2014). *DDoS Attacks Against Global Markets*.

Akerlof, G. A. (1970). The Market for "Lemons": Quality Uncertainty and the Market Mechanism. *The Quarterly Journal of Economics*, *84*(3), 488. doi:10.2307/1879431

Al-Humaigani, M., & Dunn, D. B. (2003). A model of return on investment for information systems security. In *2003 46th Midwest Symposium on Circuits and Systems* (Vol. 1, pp. 483–485). IEEE. doi:10.1109/MWSCAS.2003.1562323

Amoroso, E. G. (2011). Cyber attacks: awareness. *Network Security*, *2011*(1), 10–16. doi:10.1016/S1353-4858(11)70005-8

Anderson, R. (2001). Why information security is hard - an economic perspective. In *Seventeenth Annual Computer Security Applications Conference* (pp. 358–365). New Orleans, Louisiana: IEEE Computer Society. doi:10.1109/ACSAC.2001.991552

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M. J. G., Levi, M., … Savage, S. (2013). Measuring the Cost of Cybercrime. In R. Böhme (Ed.), *The Economics of Information Security and Privacy* (pp. 265–300). Berlin, Heidelberg: Springer Berlin Heidelberg. doi:10.1007/978-3-642-39498-0

Anderson, R., & Fuloria, S. (2010). Security Economics and Critical National Infrastructure. In T. Moore, D. Pym, & C. Ioannidis (Eds.), *Economics of Information Security and Privacy* (pp. 55–66). Boston, MA: Springer US. doi:10.1007/978-1-4419-6967-5

Anderson, R., & Moore, T. (2006). The Economics of Information Security. *Science, New Series*, *314*(5799), 610–613.

Anderson, R., & Moore, T. (2007). Information Security Economics – and Beyond. In A. Menezes (Ed.), *Advances in Cryptology - CRYPTO 2007* (Vol. 4622, pp. 68–91). Berlin, Heidelberg: Springer Berlin Heidelberg. doi:10.1007/978-3-540-74143-5

Anderson, R., & Moore, T. (2009). Information security: where computer science, economics and psychology meet. *Philosophical Transactions. Series A, Mathematical, Physical, and Engineering Sciences*, *367*(1898), 2717–27. doi:10.1098/rsta.2009.0027

Andress, A. (2004). *Surviving Security: How to Integrate People, Process, and Technology* (Second Edi.). Boca Raton, FL: CRC Press.

Arbor Networks. (2014). *Worldwide Infrastructure Security Report*.

Arora, A., Hall, D., Piato, C. A., Ramsey, D., & Telang, R. (2004). Measuring the risk-based value of IT security solutions. *IT Professional*. doi:10.1109/MITP.2004.89

Barrett, M. I. (1999). Challenges of EDI adoption for electronic trading in the London Insurance Market. *European Journal of Information Systems*.

Becker, G. S. (1968). Crime and Punishment: An Economic Approach. *Journal of Political Economy*, *76*(2), 169–217. doi:10.1086/259394

Berinato, S. (2002). Finally, a Real Return on Security Spending. *CIO Magazine*. Retrieved December 10, 2014, from http://www.cio.com.au/article/52650/finally_real_return_security_spending/

Bidou, R. (2005). Security operation center concepts & implementation.

Blue, V. (2013). Anonymous posts over 4000 U.S. bank executive credentials. Retrieved October 15, 2014, from http://www.zdnet.com/anonymous-posts-over-4000-u-s-bank-executive-credentials-7000010740/

Böhme, R., & Moore, T. (2013). *Security Metrics and Security Investment*.

Bojanc, R., & Jerman-Blažič, B. (2008a). An economic modelling approach to information security risk management. *International Journal of Information Management*, *28*(5), 413–422. doi:10.1016/j.ijinfomgt.2008.02.002

Bojanc, R., & Jerman-Blažič, B. (2008b). Towards a standard approach for quantifying an ICT security investment. *Computer Standards & Interfaces*, *30*(4), 216–222. doi:10.1016/j.csi.2007.10.013

Bowles, M. (2012). The Business of Hacking and Birth of an Industry. *Bell Labs Technical Journal*, *17*(3), 5–16. doi:10.1002/bltj.21555

Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches : empirical evidence from the stock. *Journal of Computer Security - IFIP 2000*, *11*(3), 431–448.

Carnegie Mellon University. (2014). CSIRT Services. Retrieved December 25, 2014, from http://www.cert.org/incident-management/services.cfm#note2

Casey, D. (2008). Turning log files into a security asset. *Network Security*, *2008*(2), 4–7. doi:10.1016/S1353-4858(08)70016-3

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The Effect of Internet Security Breach Announcements on Market Value : Capital Market Reactions for Breached Firms and Internet Security Developers. *International Journal of Electronic Commerce*, *9*(1), 70–104.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2005). The Value of Intrusion Detection Systems in Information Technology Security Architecture. *Information Systems Research*, *16*(1), 28–46. doi:10.1287/isre.1050.0041

Chai, S., Kim, M., & Rao, H. R. (2011). Firms' information security investment decisions: Stock market evidence of investors' behavior. *Decision Support Systems*, *50*(4), 651–661. doi:10.1016/j.dss.2010.08.017

Chen, I. J., & Popovich, K. (2003). Understanding customer relationship management (CRM). *Business Process Management Journal*, *9*(5), 672–688. doi:10.1108/14637150310496758

Cheng, T. C. E., Lam, D. Y. C., & Yeung, A. C. L. (2006). Adoption of internet banking: An empirical study in Hong Kong. *Decision Support Systems*, *42*(3), 1558–1572. doi:10.1016/j.dss.2006.01.002

Choo, K.-K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & Security*, *30*(8), 719–731. doi:10.1016/j.cose.2011.08.004

Clayton, R. (2010). Internet Multi-Homing Problems: Explanations from Economics. In T. Moore, D. Pym, & C. Ioannidis (Eds.), *Economics of Information Security and Privacy* (pp. 67–78). Boston, MA: Springer US. doi:10.1007/978-1-4419-6967-5

Cohen, J. (1992). A power primer. *Psychological Bulletin*, *112*(1), 155–159. doi:10.1037/0033-2909.112.1.155

Craig MacKinlay, A. (1997). Event Studies in Economics and Finance. *Journal of Economic Literature*, *35*(1), 13–39.

Davidson, E. (2002). Technology Frames and Framing: A Socio-Cognitive Investigation of Requirements Determination. *MIS Quarterly*, *26*(4), 329–358. doi:10.2307/4132312

Davidson, E. (2006). A Technological Frames Perspective on Information Technology and Organizational Change. *The Journal of Applied Behavioral Science*. doi:10.1177/0021886305285126

Dehning, B., Richardson, V. J., & Zmud, R. W. (2003). The Value Relevance of Announcements of Transformational Information Technology Investments. *MIS Quarterly*, *27*(4), 637–656. doi:10.2307/30036551

Delgado-Ballester, E., & Luis Munuera-Alemán, J. (2005). Does brand trust matter to brand equity? *Journal of Product & Brand Management*, *14*(3), 187–196. doi:10.1108/10610420510601058

Department for Business Innovation and Skills. (2014). *2014 INFORMATION SECURITY BREACHES SURVEY*.

Derrick Huang, C., Hu, Q., & Behara, R. S. (2008). An economic analysis of the optimal information security investment in the case of a risk-averse firm. *International Journal of Production Economics*, *114*(2), 793–804. doi:10.1016/j.ijpe.2008.04.002

Detica. (2011). *THE COST OF CYBER CRIME*. Surrey.

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Journal of Information Security*, *04*(02), 92–100. doi:10.4236/jis.2013.42011

Douligeris, C., & Mitrokotsa, A. (2004). DDoS attacks and defense mechanisms: classification and state-of-the-art. *Computer Networks*, *44*(5), 643–666. doi:10.1016/j.comnet.2003.10.003

Dunn, J. E. (2012). Hacktivists DDoS UK, US and Swedish Government websites. *TECHWORLD*. Retrieved October 15, 2014, from http://news.techworld.com/security/3379510/hacktivists-ddos-uk-us-and-swedish-government-websites/

Emm, D. (2013). *THE THREAT LANDSCAPE A practical guide from the Kaspersky Lab experts*.

ENISA. (2013a). *ENISA Threat Landscape 2013 Overview of current and emerging cyber-threats*. Heraklion, Greece. doi:10.2788/14231

ENISA. (2013b). *ENISA Threat Landscape, Mid-year 2013*. Heraklion, Greece.

European Comission. (2012). *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)* (Vol. 0011). Brussels.

European Comission. (2014). MEMO 14/186: Progress on EU data protection reform now irreversible following European Parliament vote. Strasbourg.

Fama, E. F. (1970). Efficient Capital Markets: A Review of Theory and Empirical Work. *The Journal of Finance*, *25*(2), 383. doi:10.2307/2325486

Field, A. (2013). *Discovering Statistics using IBM SPSS Statistics Fourth Edition* (Fourth Edi.). London, GB: SAGE Publications Ltd.

Fitzgerald, T. (2011). *Information Security Governance Simplified From the Boardroom to the Keyboard*. Boca Raton, FL: CRC Press.

Florêncio, D., & Herley, C. (2013). Sex, Lies and Cyber-Crime Surveys. In B. Schneier (Ed.), *Economics of Information Security and Privacy III* (pp. 35–53). New York, NY: Springer New York. doi:10.1007/978-1-4614-1981-5_3

Forrester Research Inc. (2013). *Security Operations Center (SOC) Staffing*.

Forte, D. (2003). An Inside Look at Security Operation Centres. *Network Security*, *2003*(5), 11–12. doi:10.1016/S1353-4858(03)00509-9

Forte, D. (2004). The “ART” of log correlation: part 1: Tools and techniques for correlating events and log files. *Computer Fraud & Security*, *2004*(6), 7–11.

Forte, D. (2008). An integrated approach to security incident management. *Network Security*, *2008*(2), 14–16.

Forum of Incident Response and Security Teams. (2014). *FIRST Site Visit - Requirements and Assessment (version 2.5)*. North Carolina.

Franklin, J., & Perrig, A. (2007). An inquiry into the nature and causes of the wealth of internet miscreants. In *Proceedings of the 14th ACM conference on Computer and communications security - CCS ’07* (pp. 375–388). New York, New York, USA: ACM Press. doi:10.1145/1315245.1315292

F-Secure. (2014). *Threat report H1 2014*.

Gao, X., Zhong, W., & Mei, S. (2013). A differential game approach to information security investment under hackers' knowledge dissemination. *Operations Research Letters*, *41*(5), 421–425. doi:10.1016/j.orl.2013.05.002

García-Teodoro, P., Díaz-Verdejo, J., Maciá-Fernández, G., & Vázquez, E. (2009). Anomaly-based network intrusion detection: Techniques, systems and challenges. *Computers & Security*, *28*(1-2), 18–28. doi:10.1016/j.cose.2008.08.003

Garg, A., Curtis, J., & Halper, H. (2003). Quantifying the financial impact of IT security breaches. *Information Management & Computer Security*, *11*(2), 74–83. doi:10.1108/09685220310468646

Gatzlaff, K. M., & McCullough, K. a. (2010). The Effect of Data Breaches on Shareholder Wealth. *Risk Management and Insurance Review*, *13*(1), 61–83. doi:10.1111/j.1540-6296.2010.01178.x

Gogolin, G. (2010). The Digital Crime Tsunami. *Digital Investigation*, *7*(1-2), 3–8. doi:10.1016/j.diin.2010.07.001

Goodall, J. R., Lutters, W. G., & Komlodi, A. (2009). Developing expertise for network intrusion detection. *Information Technology & People*, *22*(2), 92–108. doi:10.1108/09593840910962186

Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security*, *5*(4), 438–457. doi:10.1145/581271.581274

Gordon, L. A., Loeb, M. P., & Zhou, L. (2011). The impact of information security breaches : Has there been a downward shift in costs ? *Journal of Computer Security*, *19*(1), 33–56. doi:10.3233/JCS-2009-0398

Haight, T. (2014). The Importance of Process in Your Security Operations Center (SOC). Retrieved September 24, 2014, from http://researchcenter.paloaltonetworks.com/2014/09/importance-process-security-operations-center-soc/

Hämmerli, B. (2012). Financial Services Industry. In J. Lopez, R. Setola, & S. D. Wolthusen (Eds.), *Critical Infrastructure Protection* (Vol. 7130, pp. 301–329). Berlin, Heidelberg: Springer Berlin Heidelberg. doi:10.1007/978-3-642-28920-0_13

Hanna, A., & Rance, S. (2011). *ITIL® glossary and abbreviations*.

Harkins, M. (2012). *Managing Risk and Information Security: Protect to Enable*. (J. Pepper & D. Stuart, Eds.). New York, NY: Apress Media.

Hausken, K. (2006). Returns to information security investment: The effect of alternative information security breach functions on optimal investment and sensitivity to vulnerability. *Information Systems Frontiers*, *8*(5), 338–349. doi:10.1007/s10796-006-9011-6

Hausken, K. (2012). Returns to information security investment: Endogenizing the expected loss. *Information Systems Frontiers*, *16*(2), 329–336. doi:10.1007/s10796-012-9390-9

Hewlett-Packard. (2009). *Security operations Building a successful SOC*. doi:10.1109/9780470546390.part5

Hewlett-Packard. (2011a). *Building a successful security operations center*.

Hewlett-Packard. (2011b). *DEMONSTRATING THE ROI FOR SIEM Tales from the Trenches*.

Hewlett-Packard. (2013). *5G / SOC : SOC Generations*.

Hoppmann, J., Diaz Anadon, L., & Narayanamurti, V. (2014). How Technological Frames and Focus Co-Evolve with the Organizational Environment. *Academy of Management Proceedings*, *2014*(1), 10665–10665.

Horne, B. (2014). On Computer Security Incident Response Teams. *IEEE Security & Privacy*, *12*(5), 13–15. doi:10.1109/MSP.2014.96

Hovav, A., & D'Arcy, J. (2003). The Impact of Denial-of-Service Attack Announcements on the Market Value of Firms. *Risk Management and Insurance Review*, *6*(2), 97–121. doi:10.1046/J.1098-1616.2003.026.x

Hovav, A., & D'Arcy, J. (2004). The Impact of Virus Attack Announcements on the Market Value of Firms. *Information Systems Security*, *13*(3), 32–40. doi:10.1201/1086/44530.13.3.20040701/83067.5

Hovav, A., & Gray, P. (2014). The Ripple Effect of an Information Security Breach Event: A Stakeholder Analysis. *Communications of the Association for Information Systems Volume*, *34*(1), 893–912.

Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. *Leading Issues in Information Warfare & Security Research*, *1*(2011), 1–14.

Hyman, P. (2013). Cybercrime: It's Serious, But Exactly How Serious? *Communications of the ACM*, *56*(3), 18. doi:10.1145/2428556.2428563

Iansiti, M., & Levien, R. (2004). *The Keystone Advantage: What the New Dynamics of Business Ecosystems Mean for Strategy, Innovation, and Sustainability*. Boston, MA: Harvard Business School Press.

IBM. (2013). *The economics of IT risk and reputation*. Somers, NY.

IBM Global Technology Services. (2013). *Strategy considerations for building a security operations center*. Somers, NY.

ICS-CERT. (2013). *ICS-CERT MONITOR*.

Im, K. S., Dow, K. E., & Grover, V. (2001). Research Report: A Reexamination of IT Investment and the Market Value of the Firm—An Event Study Methodology. *Information Systems Research*, *12*(1), 103–117. doi:10.1287/isre.12.1.103.9718

ISO. (2009). ISO/IEC 15408-1:2009 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model. Geneva, SW: International Organization for Standardization.

ISO/IEC. (2012). *ISO/IEC 27000 Information technology —Security techniques —Information security management systems — Overview and vocabulary*. Geneva, SW.

Jacobs, P., Arnab, A., & Irwin, B. (2013). Classification of Security Operation Centers. In *2013 Information Security for South Africa* (pp. 1–7). Johannesburg, South Africa: IEEE. doi:10.1109/ISSA.2013.6641054

Kamra, A., Bertino, E., & Nehme, R. (2008). Responding to Anomalous Database Requests. In W. Jonker & M. Petković (Eds.), *Secure Data Management* (Vol. 5159, pp. 50–66). Berlin, Heidelberg: Springer Berlin Heidelberg. doi:10.1007/978-3-540-85259-9

Karim Ganame, A., Bourgeois, J., Bidou, R., & Spies, F. (2008). A global security architecture for intrusion detection on computer networks. *Computers & Security*, *27*(1-2), 30–47. doi:10.1016/j.cose.2008.03.004

Kaspersky Labs. (2013). *THE EVOLUTION OF PHISHING ATTACKS: 2011-2013*.

Kelley, D., & Moritz, R. (2006). Best Practices for Building a Security Operations Center. *Information Systems Security*, *14*(6), 27–32. doi:10.1201/1086.1065898X/45782.14.6.20060101/91856.6

Kim, W., Jeong, O.-R., Kim, C., & So, J. (2011). The dark side of the Internet: Attacks, costs and responses. *Information Systems*, *36*(3), 675–705. doi:10.1016/j.is.2010.11.003

Koivunen, E. (2012). "Why Wasn't I Notified?": Information Security Incident Reporting Demystified. In T. Aura, K. Järvinen, & K. Nyberg (Eds.), *Information Security Technology for Applications* (Vol. 7127, pp. 55–70). Berlin, Heidelberg: Springer Berlin Heidelberg. doi:10.1007/978-3-642-27937-9_5

Kotov, V., & Massacci, F. (2013). Anatomy of Exploit Kits. In J. Jürjens, B. Livshits, & R. Scandariato (Eds.), *Engineering Secure Software and Systems* (Vol. 7781, pp. 181–196). Berlin, Heidelberg: Springer Berlin Heidelberg. doi:10.1007/978-3-642-36563-8

Krebs, B. (2009). Sprint: Employee Stole Customer Data. *The Washington Post*.

Krebs, B. (2013). DDoS Attack on Bank Hid $900,000 Cyberheist - Krebs On Secuirty. Retrieved from http://krebsonsecurity.com/2013/02/ddos-attack-on-bank-hid-900000-cyberheist/

Kruidhof, O. (2014). Evolution of National and Corporate CERTs–Trust, the Key Factor. In *Best Practices in Computer Network Defense: Incident Detection and Response* (pp. 81–96). doi:10.3233/978-1-61499-372-8-81

Kulikova, O., Heil, R., van den Berg, J., & Pieters, W. (2012). Cyber Crisis Management: A Decision-Support Framework for Disclosing Security Incident Information. In *2012 International Conference on Cyber Security* (pp. 103–112). Washington, DC: IEEE. doi:10.1109/CyberSecurity.2012.20

Larsen, K. R., Allen, G., & Eargle, D. (2015). Theories Used in IS Research Wiki. *Theories Used in IS Research Wiki*. Retrieved April 20, 2015, from http://is.theorizeit.org

Lee, Y. J., Kauffman, R. J., & Sougstad, R. (2011). Profit-maximizing firm investments in customer information security. *Decision Support Systems*, *51*(4), 904–920. doi:10.1016/j.dss.2011.02.009

Lesk, M. (2007). The New Front Line: Estonia under Cyberassault. *IEEE Security & Privacy Magazine*, *5*(4), 76–79. doi:10.1109/MSP.2007.98

Leuthesser, L., Kohli, C. S., & Harich, K. R. (1995). Brand equity: the halo effect measure. *European Journal of Marketing*, *29*(4), 57–66. doi:10.1108/03090569510086657

Li, J. J., Hsieh, C. C., & Lin, H. H. (2013). A hierarchical mobile-agent-based security operation center. *International Journal of Communication Systems*, *26*(12), 1503–1519. doi:10.1002/dac

Lin, C., Wong, H., & Wu, T. (2005). Enhancing interoperability of security operation center to heterogeneous intrusion detection systems. In *Proceedings 39th Annual 2005 International Carnahan Conference on Security Technology* (pp. 216–221). Las Palmas, Spain: IEEE. doi:10.1109/CCST.2005.1594841

Luthra, K., Sharma, A., Gahlot, D., & Gahlot, A. (2013). ARMING YOUR SECURITY OPERATIONS CENTER WITH THE RIGHT TECHNOLOGY & SERVICES. *International Journal of Computer Science and Management Research*, *2*(5), 2312–2314.

Madani, A., Rezayi, S., & Gharaee, H. (2011). Log management comprehensive architecture in Security Operation Center (SOC). In *2011 International Conference on Computational Aspects of Social Networks (CASoN)* (pp. 284–289). Salamanca, Spain: IEEE. doi:10.1109/CASON.2011.6085959

Malecki, F. (2013). Defending your business from exploit kits. *Computer Fraud & Security*, *2013*(6), 19–20. doi:10.1016/S1361-3723(13)70056-3

Manky, D. (2013). Cybercrime as a service: a very modern business. *Computer Fraud & Security*, *2013*(6), 9–13. doi:10.1016/S1361-3723(13)70053-8

McAfee. (2012). *Creating and Maintaining a SOC - The details behind successful Security Operations Centers*. Santa Clara, CA.

Mcafee. (2013). *McAfee Threats Report: First Quarter 2013*. Santa Clara, CA.

McAffee. (2009). *Virtual Criminology Report 2009 Virtually Here: The Age of Cyber Warfare*. Santa Clara, CA.

McWilliams, A., & Siegel, D. (1997). Event Studies in Management Research: Theoretical and Empirical Issues. *The Academy of Management Journal*, *40*(3), 626–657.

Mizzi, A. (2010). Return on Information Security Investment-The Viability Of An Anti-Spam Solution In A Wireless Environment. *International Journal of Network Security*, *10*(1), 18–24.

Moore, D., Paxson, V., & Savage, S. (2003). Inside the slammer worm. *IEEE Security and Privacy*, *1*(4), 33–39.

Moore, T., & Clayton, R. (2007). Examining the impact of website take-down on phishing. In L. F. Cranor (Ed.), *Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit on - eCrime '07* (pp. 1–13). New York, New York, USA: ACM Press. doi:10.1145/1299015.1299016

Moore, T., Clayton, R., & Anderson, R. (2009). The economics of online crime. *The Journal of Economic Perspectives*, *23*(3), 3–20.

NASA SOC. (2010). *Anatomy of a Security Operations Center*.

National Cyber Security Centre. (2013). *Cyber Security Assessment Netherlands CSAN-3*. The Hague.

National Vulnerability Database. (2014). NVD - Statistics Page. Retrieved from http://web.nvd.nist.gov/view/vuln/statistics

Neuhaus, S., & Plattner, B. (2013). Software Security Economics: Theory, in Practice. In R. Böhme (Ed.), *The Economics of Information Security and Privacy* (pp. 75–92). Berlin, Heidelberg: Springer Berlin Heidelberg. doi:10.1007/978-3-642-39498-0

Neumeier, M. (2005). *The Brand Gap: How to Bridge the Distance Between Business Strategy and Design*. Berkeley, CA: New Riders Publishing.

Nicolett, M., & Kavanagh, K. M. (2011). *Magic Quadrant for Security Information and Event Management Gartner Research Note G00212454*.

NIST. (2012). *NIST Special Publication 800-30 Rev. 1 - Guide for Conducting Risk Assessments*. Gaithersburg, MD.

Nkhoma, M. Z., Jahankhani, H., & Mouratidis, H. (2007). Information and network management security Investment. In *Advances in Computing and Technology, The School of Computing and Technology 2nd Annual Conference* (pp. 89–100). London.

Obama, B. (2009). REMARKS BY THE PRESIDENT ON SECURING OUR NATION'S CYBER INFRASTRUCTURE. Retrieved from http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/

Olesen, K. (2014). Implications of dominant technological frames over a longitudinal period. *Information Systems Journal*, *24*(3), 207–228. doi:10.1111/isj.12006

Orlikowski, W. J., & Gash, D. C. (1994). Technological frames: making sense of information technology in organizations. *ACM Transactions on Information Systems*, *12*(2), 174–207. doi:10.1145/196734.196745

Osborne, J. W. (2002). Notes on the use of data transformations. *Practical Assessment, Research & Evaluation*, *8*(6), 1–8.

Patel, A., Qassim, Q., & Wills, C. (2010). A survey of intrusion detection and prevention systems. *Information Management & Computer Security*, *18*(4), 277–290. doi:10.1108/09685221011079199

Pavlou, P. A., Liang, H., & Xue, Y. (2007). Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principal- Agent Perspective. *MIS Quarterly*, *31*(1), 105–136.

Pearson, N. (2014). A larger problem: financial and reputational risks. *Computer Fraud & Security*, *2014*(4), 11–13. doi:10.1016/S1361-3723(14)70480-4

Pee, L. G., & Kankanhalli, A. (2009). A Model of Organisational Knowledge Management Maturity Based on People, Process, and Technology. *Journal of Information & Knowledge Management*, *08*(02), 79–99. doi:10.1142/S0219649209002270

Peter, G. (2014). *Stopping Zero-Day Exploits For Dummies®, Trusteer Special Edition*. Hoboken, NJ: John Wiley & Sons, Inc.

Pilling, R. (2013). Global threats, cyber-security nightmares and how to protect against them. *Computer Fraud & Security*, *2013*(9), 14–18. doi:10.1016/S1361-3723(13)70081-2

Pirounias, S., Mermigas, D., & Patsakis, C. (2014). The relation between information security events and firm market value, empirical evidence on recent disclosures: An extension of the GLZ study. *Journal of Information Security and Applications*, *19*(4-5), 257–271. doi:10.1016/j.jisa.2014.07.001

Ponemon Institute. (2013). *2013 Cost of Data Breach Study: Global Analysis Benchmark*.

Ponemon Institute. (2014). *2014 Cost of Data Breach Study: Global Analysis*. Traverse City, Michigan.

Potts, M. (2012). The state of information security. *Network Security*, *2012*(7), 9–11. doi:10.1016/S1353-4858(12)70064-8

Prodan, M., Prodan, A., & Purcarea, A. (2015). Three New Dimensions to People, Process, Technology Improvement Model. In A. Rocha, A. M. Correia, S. Costanzo, & L. P. Reis (Eds.), *New Contributions in Information Systems and Technologies SE - 47* (Vol. 353, pp. 481–490). Springer International Publishing. doi:10.1007/978-3-319-16486-1_47

Purser, S. a. (2004). Improving the ROI of the security management process. *Computers & Security*, *23*(7), 542–546. doi:10.1016/j.cose.2004.09.004

PWC. (2014). *Defending yesterday: Key findings from The Global State of Information Security ® Survey 2014*.

Q1 Labs. (2009). *The Business Case for a Next-Generation SIEM: Delivering operational efficiency and lower costs through an integrated approach to network security management Copyright*. Waltham, MA, USA.

Rahrovani, Y., & Pinsonneault, A. (2012). On the Business Value of Information Technology: A Theory of Slack Resources. In Y. K. Dwivedi, M. R. Wade, & S. L. Schneberger (Eds.), *Information Systems Theory* (Vol. 28, pp. 165–198). New York, NY: Springer New York. doi:10.1007/978-1-4419-6108-2

Rainer, R. K. (2008). An Overview of Threats to Information Security. In M. Khosrow-Pour (Ed.), *Encyclopedia of Information Science and Technology, Second Edition* (pp. 2990–2995). Hershey, PA: IGI Global. doi:10.4018/978-1-60566-026-4

Ranganathan, C., & Brown, C. V. (2006). ERP Investments and the Market Value of Firms: Toward an Understanding of Influential ERP Project Variables. *Information Systems Research*, *17*(2), 145–161. doi:10.1287/isre.1060.0084

Rescorla, E. (2005). Is finding security holes a good idea? *IEEE Security and Privacy Magazine*, *3*(1), 14–19. doi:10.1109/MSP.2005.17

Richards, K. (2009). *The Australian Business Assessment of Computer User Security (ABACUS): A national survey.* Canberra: Australian Institute of Criminology.

Rob, T., & Martin, J. (2006). The underground economy: priceless. *The USENIX Magazine*, *31*(6), 7–16.

Robinson, N., Gribbon, L., Horvath, V., & Robertson, K. (2013). *Cyber-security threat characterisation A rapid comparative analysis*. Santa Monica, CA.

RSA Security. (2009). *ROI and SIEM: How the RSA enVision Platform Delivers an Industry-Leading ROI*.

Ryan, J. J. C. H., Mazzuchi, T. a., Ryan, D. J., Lopez de la Cruz, J., & Cooke, R. (2012). Quantifying information security risks using expert judgment elicitation. *Computers & Operations Research*, *39*(4), 774–784. doi:10.1016/j.cor.2010.11.013

Sabherwal, R., & Sabherwal, S. (2005). Knowledge Management Using Information Technology: Determinants of Short-Term Impact on Firm Value*. *Decision Sciences*, *36*(4), 531–567. doi:10.1111/j.1540-5414.2005.00102.x

Sanford, C., & Bhattacherjee, A. (2008). IT Implementation in a Developing Country Municipality. *International Journal of Technology and Human Interaction*, *4*(3), 68–93. doi:10.4018/jthi.2008070104

Scarfone, K., & Mell, P. (2007). *Guide to Intrusion Detection and Prevention Systems (IDPS) Recommendations of the National Institute of Standards and Technology*. Gaithersburg, MD.

Shackelford, S. J. (2012). Should your firm invest in cyber risk insurance? *Business Horizons*, *55*(4), 349–356. doi:10.1016/j.bushor.2012.02.004

Shameli-Sendi, A., Cheriet, M., & Hamou-Lhadj, A. (2014). Taxonomy of intrusion risk assessment and response system. *Computers & Security*, *45*, 1–16. doi:10.1016/j.cose.2014.04.009

Snow, G. M. (2011). *CYBER SECURITY: THREATS TO THE FINANCIAL SECTOR STATEMENT OF GORDON M. SNOW ASSISTANT DIRECTOR CYBER DIVISION FEDERAL BUREAU OF INVESTIGATION*. US Department of Justice.

Sonnenreich, W. (2006). Return On Security Investment (ROSI): A Practical Quantitative Model. *Journal of Research and Practice in Information Technology*, *38*(1), 45–56.

Sood, A. K., & Enbody, R. (2012). Targeted Cyber Attacks - A Superset of Advanced Persistent Threats. *IEEE Security & Privacy*, *11*(1), 54–61. doi:10.1109/MSP.2012.90

Sood, A. K., & Enbody, R. J. (2013). Crimeware-as-a-service—A survey of commoditized crimeware in the underground market. *International Journal of Critical Infrastructure Protection*, *6*(1), 28–38. doi:10.1016/j.ijcip.2013.01.002

Stoll, M. (2013). Stakeholder Oriented Information Security Reporting. In K. Elleithy & T. Sobh (Eds.), *Innovations and Advances in Computer, Information, Systems Sciences, and Engineering* (Vol. 152, pp. 241–252). New York, NY: Springer New York. doi:10.1007/978-1-4614-3535-8

Stolze, M., Pawlitzek, R., & Wespi, A. (2003). Visual Problem-Solving Support for New Event Triage in Centralized Network Security Monitoring: Challenges, Tools and Benefits. In *IT-Incident Management & IT-Forensics* (pp. 67–76). Stuttgart, DE.

Suby, M. (2013). *The 2013 (ISC)2 Global Information Security Workforce Study*. Mountain View, CA.

Symantec. (2014). *INTERNET SECURITY THREAT REPORT 2014* (Vol. 19). Mountain View, CA.

The Commission on the Theft of American Intellectual Property. (2013). *THE IP COMMISSION REPORT*.

Thomson, G. (2011). APTs: a poorly understood challenge. *Network Security*, *2011*(11), 9–11. doi:10.1016/S1353-4858(11)70118-0

Tsiakis, K. T., & Pekos, G. D. (2008). Analysing and determining Return on Investment for Information Security. In *International Conference on Applied Economics – ICOAE 2008* (pp. 879–883).

Tsiakis, T., & Stephanides, G. (2005). The economic approach of information security. *Computers & Security*, *24*(2), 105–108. doi:10.1016/j.cose.2005.02.001

U.S. Department of Energy, Office of Inspector General, & Office of Audits and Inspections. (2013). *The Department of Energy's July 2013 Cyber Security Breach*. Washington, DC.

U.S. Government Accountability Office. (2015). Ensuring the Security of Federal Information Systems and Cyber Critical Infrastructure and Protecting the Privacy of Personally Identifiable Information. *High Risk Series*. Retrieved from http://www.gao.gov/highrisk/protecting_the_federal_government_information_systems/why_did_study#t=1

United States Government. U.S. Code, Pub. L. No. §§ 2543 (2013). United States.

US CERT. (2013). Cryptolocker Ransomware Infections. Retrieved October 17, 2014, from https://www.us-cert.gov/ncas/alerts/TA13-309A

Van De Weerd, I., & Brinkkemper, S. (2008). Handbook of Research on Modern Systems Analysis and Design Technologies and Applications. In M. Syed & S. Syed (Eds.), *Handbook of Research on Modern Systems Analysis and Design Technologies and Applications* (pp. 35–54). Hershey, PA: IGI Global. doi:10.4018/978-1-59904-887-1

Verizon. (2012). *2012 DATA BREACH INVESTIGATIONS REPORT*.

Vinhas Da Silva, R., & Faridah Syed Alwi, S. (2008). Online brand attributes and online corporate brand images. *European Journal of Marketing*, *42*(9/10), 1039–1058. doi:10.1108/03090560810891136

Walker, S. (2012). Economics and the cyber challenge. *Information Security Technical Report*, *17*(1-2), 9–18. doi:10.1016/j.istr.2011.12.003

Wang, J., Chaudhury, A., & Rao, H. R. (2008). Research Note —A Value-at-Risk Approach to Information Security Investment. *Information Systems Research*, *19*(1), 106–120. doi:10.1287/isre.1070.0143

Wang, S., Zhang, Z., & Kadobayashi, Y. (2013). Exploring attack graph for cost-benefit security hardening: A probabilistic approach. *Computers & Security*, *32*(2), 158–169. doi:10.1016/j.cose.2012.09.013

Ward, J., & Peppard, J. (2007). *Strategic planning for information systems*. (R. Boland & R. Hirschheim, Eds.) (Third.). Chichester: John Wiley & Sons Ltd.

Whitman, M. (2003). Enemy at the gate: threats to information security. *Communications of the ACM*, *46*(8), 91–95.

Whittaker, B. (1999). What went wrong? Unsuccessful information technology projects. *Information Management & Computer Security*, *7*(1), 23–30. doi:10.1108/09685229910255160

Willemson, J. (2010). Extending the Gordon and Loeb Model for Information Security Investment. In *2010 International Conference on Availability, Reliability and Security* (pp. 258–261). IEEE. doi:10.1109/ARES.2010.37

Wood, C. C., & Parker, D. B. (2004). Why ROI and similar financial tools are not advisable for evaluating the merits of security projects. *Computer Fraud & Security*, *2004*(5), 8–10. doi:10.1016/S1361-3723(04)00064-8

Wortham, J. (2009). For Sprint Nextel, a Drop in Customers and Earnings. *The New York Times*. New York, NY.

Wu, S.-I., & Jang, J.-Y. (2013a). The impact of ISO certification on consumers' purchase intention. *Total Quality Management & Business Excellence*, *25*(3-4), 412–426. doi:10.1080/14783363.2013.776770

Wu, S.-I., & Jang, J.-Y. (2013b). The performance of ISO certification based on consumer perspective: A case study of a travel agency. *Total Quality Management & Business Excellence*, *24*(3-4), 496–518. doi:10.1080/14783363.2011.560704

Zimmerman, C. (2014). *Ten Strategies of a World-Class Cybersecurity Operations Center*. Bedford, MA: MITRE Corporate Communications and Public Affairs.

Appendices

Appendix A – Preliminary SOC Related Literature Search

This appendix summarizes the method and results of the preliminary literature search indicating the lack of a business perspective when it comes to Security Operation Centers. The search was performed using Utrecht University's access rights.

Table A.1 summarizes the database used and the input given:

Database	Input 1	Input 2	Input 3	Input 4	Type of Input	Boolean Connector	Present in
Google Scholar	Security Operation Center	Security Operations Center	Security Operation Centre	Security Operations Centre	Exact Phrase	OR	Title Of Paper

Table A.1: Database and Input of Preliminary SLR

Table A.2 summarizes the found literature and highlights whether it had a technical or business focus.

Title	Authors	Year	Technical Or Business Focus
Security operation center concepts & implementation	R Bidou	2005	Technical
Security operation center based on immune system	Y Niu, Q Zhang, QL Zheng, H Peng	2007	Technical
Security operation center design based on DS evidence theory	X Hu, C Xie	2006	Technical
Best Practices for Building a Security Operations Center	D Kelley, R Moritz	2006	Business
Managing Security of Grid Architecture with a Grid Security Operation Center.	J Bourgeois, RH Syed	2009	Technical
Log management comprehensive architecture in Security Operation Center (SOC)	A Madani, S Rezayi, H Gharaee	2011	Technical
Enhancing interoperability of security operation center to heterogeneous intrusion detection systems	ACC Lin, HK Wong, TC Wu	2005	Technical
A hierarchical mobile-agent-based security operation center	JS Li, CJ Hsieh, HY Lin	2013	Technical
Design on Response mechanism of Security Operations Center based on ITIL	L Bao-ling, C Bao-xiang	2013	Not Known – Access Denied
The security operations center based on correlation analysis	S Yuan, C Zou	2011	Technical
Establish Security Operation Center (SOC) Based on Security Domain [J]	Z Zhibo	2006	Technical
Research on key technologies of network security operations centre [J]	B ZHAO, Y WANG, N XU, L LI	2009	Technical
The analysis of event correlation in security operations center	D Zhang, D Zhang	2011	Technical
Research on Security Operations Center Technology Based on Cloud Computing	LWC Baoxiang	2011	Technical
Design and Implementation of Mini-Security Operation Center for Enterprise	SM Leu	2005	Technical
ARMING YOUR SECURITY OPERATIONS CENTER WITH THE RIGHT TECHNOLOGY & SERVICES	K Luthra, A Sharma, D Gahlot, A Gahlot	2013	Both

Cyber security operations center characterization model and analysis	S Kowtha, LA Nolan, RA Daley	2012	Not Known - Access Denied
Implementation of the distributed hierarchical security operation center using mobile agent group	JS Li, CJ Hsieh	2010	Technical
Design of security operation center based on multi-agents system	Y Niu, Q Zheng, H Peng	2007	Technical
How to develop and win support for a properly equipped security operations center	JR Clark	1983	Business
Agent-Oriented Intelligent IPv6 Network Security Operation Center	PH Huang, CY Lin, CF Wang, B Tseng	2006	Technical
Deployment and Administration of Security Operation Center	C Chang	2007	Business
Description of the map board portion of the Security Operations Center of the Plutonium Protection System	CE Ringler	1979	Technical
Software Environment for Simulation and Evaluation of a Security Operation Center	J Bourgeois, AK Ganame, I Kotenko	2007	Technical

Table A.2: Results Summary

Appendix B – Forum for Incident Response and Security Teams Member Information

This appendix summarizes the information pertaining to FIRST member groups and their respective organizations.

Team name	Official Team name	Constituency	Country
Adobe PSIRT	Adobe Product Security Incident Response Team	Adobe	US
ADP CIRC	ADP CIRC	Automatic Data Processing	US
Amazon SIRT	Amazon Security Incident Response Team	Amazon	US
Apple	Apple Computer	Apple	US
AT&T	AT&T	AT&T	US
BAC-SIRT	Bank of America Computer Incident Response Team	Bank of America	US
B-CIRT	Boeing - Computing Incident Response Team	Boeing	US
Box IRT	Box Incident Reponse Team	Boc.com	US
CERT/CC	CERT Coordination Center	The Internet	US
Cisco PSIRT	Cisco Systems Product Security Incident Response Team	Cisco products	US
Cisco Systems	Cisco Systems CSIRT	Cisco	US
Citi CIRT	Citi CIRT	Citigroup	US
DIRT	DePaul Incident Response Team	DePaul University	US
eBay CERT	eBay Global Information Security Monitoring and Response Team	eBay	US
EMC	EMC's Product Security Response Center	EMC2	US
EY	Ernst & Young LLP	Ernst & Young	US
FB-SIR	Facebook Security Incident Response	Facebook	US
Fidelity IO-CERT	Fidelity Intelligence Operations CERT	Fidelity Investments (FMR LLC)	US
FSIRT	FIS Security Incident Response Team	Fidelity National Information Services	US
GD-AIS	General Dynamics - AIS	General Dynamics commercial and government customers	US
GE-CIRT	General Electric Computer Incident Response Team	General Electric	US
GIST	Google Information Security Team	Google	US
Goldman Sachs	Goldman, Sachs and Company	Goldman, Sachs offices worldwide	US

Team name	Official Team name	Constituency	Country
HP GSIRT	HP Enterprise Security - Global Security Incident Response Team	HP Trade (ITO/BPO/TS)	US
HP SSRT	HP Software Security Response Team	all HP customers (internal & external)	US
HSBC REACT	Rapid Emergency Action Crisis Team	HSBC Global	US
IBM	IBM	IBM and IBM customers	US
ICANN CIRT	Internet Corporation for Assigned Names and Numbers - Computer Incident Response Team	Internet Corporation for Assigned Names and Numbers	US
IID	Internet Identity	ICT vendor customer base	US
Intel FIRST Team	Intel FIRST Team	Intel	US
IT-ISAC	Information Technology Information Sharing and Analysis Center	The IT-ISAC is a collection of prominent IT industry vendors. Representatives from member organizations regularly share security and threat information	US
JC3-CIRC	Department of Energy Joint Cybersecurity Coordination Center	US Department of Energy, contractors	US
Juniper SIRT	Juniper Networks Security Incident Response Team	Juniper (internal and external)	US
Leidos-IRT	Leidos - Incident Response Team	Leidos Commercial and government customers	US
LG-CIRT	Lookingglass Cyber Solutions Threat Team	Any customer that has purchased our products and services for threat management.	US
LM-CIRT	Lockheed Martin Computer Incident Response Team	Lockheed Martin	US
Mandiant Security	Mandiant/FireEye	ICT vendor customer base	US
MFCIRT	McAfee Computer Incident Response Team	McAffee - Internal Only	US
MM	MarkMonitor	ICT vendor customer base	US
Morgan Stanley	Morgan Stanley Computer Emergency Response Team	Morgan Stanley	US
MSCERT	Microsoft Security Response Center Team	Internal and external Microsoft customers	US
NASA SOC	NASA Security Operations Center	NASA and the international aerospace community	US
NBCU-ISRT	NBCU-ISRT	NBCUniversal	US
NCSA-IRST	National Center for Supercomputing Applications IRST	National Center for Supercomputing Applications	US
NeuCIRT	Neustar Computer Incident Response Team	ISP Cutomer base	US

Team name	Official Team name	Constituency	Country
NIHIRT	NIH Incident Response Team	National Institutes of Health (USA)	US
NIST	NIST IT Security	National Institute of Standards and Technology (USA)	US
NOMX CERT	NASDAQ OMX CERT	NASDAQ OMX	US
NU-CERT	Northwestern University	Northwestern University Faculty/Staff/Students	US
OISIR	World Bank Group Office of Information Security Incident Response	The World Bank Group	US
ORACERT	Oracle Global Product Security	Oracle	US
OSU-IRT	The Ohio State University Incident Response Team	The Ohio State University, its faculty, staff and students; branch campuses; and affiliated organizations.	US
PayPal GSIRT	PayPal Global Security Incident Response Team	Paypal	US
PCH	Packet Clearing House	Internet community in general, particularly ccTLD operators and IXPs	US
RayCERT	Raytheon Computer Emergency Response Team	Raytheon	US
RH-ISIRT	Red Hat Information Security Incident Response Team	Red Hat	US
Salesforce CSIRT	Salesforce.com Computer Security Incident Response Team	Salesforce (internal & external)	US
Scottrade SIRT	Scottrade Security Incident Response Team	Scottrade	US
SWRX CERT	SecureWorks Computer Emergency Response Team	External to host	US
SymCERT	Symantec Computer Emergency Response Team	Symantec and customers	US
Team Cymru	Team Cymru	The team is decentralized and independent of any single legal entity therefore this field does not apply.	US
TS/ICSA FIRST	TruSecure Corporation	www.Cybertrust.com, www.TruSecure.com, www.ubizen.com, www.betrusted.com, www.ICSA.net & clients for all of the above	US
UB-First	UB-First	University at Buffalo	US
UCERT	Unisys CERT	Unisys Corpoartion internal/external users	US
UNDP ISIRT	UNDP ISIRT	United Nations Development Programme	US
US-CERT	United States Computer Emergency Readiness Center	US Critical infrastructure, US Federal civil agencies, and US state and local governments	US

Team name	Official Team name	Constituency	Country
VeriSign	Verisign	Security Services, DNS, and PKI Clients	US
Verizon	Verizon NSIRT	Verizon Employees, Contractors and Alliance Partners	US
VISA-CIRT	VISA-CIRT	VISA (worldwide)	US
WFC SOC	Wells Fargo Security Operation Center(SOC)	Wells Fargo	US
Xilinx PSIRT	Xilinx Product Security Incident Response Team	Xilinx customers (internal and external)	US
Yahoo IRT	Yahoo Incident Response Team	Support all of Yahoo environments across the world	US

Appendix C – Matched Pairs

This appendix describes in more details all of the pairings made and the rationale underlying them. In each heading the listing pertaining to a SOC and having to be matched comes first.

Education Industry Pairings

Pairing #1: Northwestern University's 2005 Breach – University of Connecticut

By searching the known breached records dataset seven matching institutions that had also been breached in 2005 by a hacking attempt were found. The records involved the California State Polytechnic, Cornell and Georgia Southern universities. Additionally, the universities of Colorado (two instances), Connecticut and Delaware were matching to the criteria defined above.

Two of the matching listings had to be dropped from the comparison. In one case (University of Delaware) the listing involved multiple breaches without specifying how stolen records were distributed among them. On the other, the description was unclear on whether the records accessed contained information about students and faculty or not. By random selection the University of Connecticut was appointed as the matched pair.

Pairing #2: Northwestern University's 2006 Breach – Universities of Texas at El Paso and Dallas

Searching the dataset produced two possible matches of same year breaches at the Universities of Texas at El Paso and Dallas. By random selection the University of Texas at El Paso was appointed as the matched pair.

Pairing #3: Ohio State University's 2007 Breach - University of Texas McCombs School of Business

In this case no similar size institution was found on the same year. Therefore the search was expanded on the previous and following years where an appropriate match was found.

Pairing #4: Ohio State University's 2010 Breach - University of Florida

Again no similar size institution was found on the same year. After the expansion of the search two possible matches were found pertaining to two breaches at the University of Florida at 2008 and 2009. The former was dismissed due to the fact that the records involved were those of patients to the university's college of dentistry and therefore fall outside the control of university population size. The latter was kept since no dismissal reason existed.

Medical Industry Pairings

Pairing #5: Ohio State University Medical Center – Two Institutions

Following the selected strategy for the medical industry two appropriate matches were found. Those were the Akron Children's Hospital and Ohio University Hudson Health Center which in 2006 had been the victims of successful hacking attempts. The reader should note that the Ohio State University and the Ohio University are different organizations. The matching organizations respectively operate at Akron and Athens, both cities with less than half the population of Columbus according to the US Census Bureau (2014). By random selection the Akron Children's Hospital was deemed the matching pair.

Finance Industry Pairings

Pairing #6: Wachovia, Bank of America, PNC Financial Services Group 2005 Breach – Compass Bank

This insider breach listing was matched by a different year, insider breach to the direct competitor Compass Bank.

Pairing #7: Fidelity National Information Services/Certegy Check Services Inc. 2007 Breach – Countrywide Financial Corp.

This insider breach listing occurred in Certegy, a subsidiary of Fidelity National Information Services which in turn is a subsidiary of Fidelity National Financial. Fidelity National Financial is the United States' largest provider of commercial and residential mortgage and diversified services. A similar company found in the dataset was Countrywide Financial Corporation who also operates within the mortgage market.

The financial industry savvy reader will know that Countrywide is now known as Bank of America Home Loans since it has been acquired by Bank of America. As stated before Bank of America operates a FIRST member SOC. This could pose a threat to the validity of the matching. The dates of the public annunciation of the breach (02/08/2008) and the acquisition (01/07/2008) however, make it safe to assume that the breach occurred before SOC services were established in the acquired company.

Pairing #8: Citibank 2008 Breach - Global Payments Inc.

This listing concerned the theft of credit card information due to illegal access to IT systems. This is important since most other card type listings involved breaches that had either skimming or ATM tampering as the method of obtaining personal information. By searching the dataset two similar breaches were found.

The first involved Global Payments Inc. a worldwide credit and debit card processor and the second West Shore bank. Due to the huge difference in organizational size compared to Citibank the latter was decided to be dropped.

Pairing #9: RBS Worldpay - CardSystems

The two firms were considered direct competitors since both are multinational payment processing companies. It is interesting to note that CardSystems undergone a buy-out shortly after its breach.

Pairing #10: Wells Fargo 2008 Breach – Davidson Companies

By searching the dataset four possible same year matches were found. One of them affecting Washington Trust Co. occurred not at the company but at an unidentified Mastercard merchant. Thus it was excluded. Moreover, a possible match relating to LPL Financial was also excluded since the company specializes in financial advisory services only. Among the remaining matches, relating to Davidson Companies and Franklin Savings and Loan, the former was kept as the paired match by means or random selection.

Pairing #11: Wells Fargo 2010 Breach – JP Morgan

This matching was the outcome of the two directly competitive companies suffering from a same type breach at the same year.

Pairing #12: Bank of America 2011 Breach – Huntington National Bank

As in the previous matching both of the listings paired involved a same type, same year breach concerning two direct competitors.

Pairing #13: Citibank 2011 Breach – JP Morgan

Again the pairing was made due to the companies being direct competitors. It must be noted that the JP Morgan breach though occurred two years later than the Citibank one.

Pairing #14: Fidelity National Information Services, Inc. 2011 Breach - Digital River Inc.

In this pairing, both firms are publicly listed technology companies with significant parts of their portfolio being centered upon payment services. They were thus considered direct competitors.

Pairing #15: Electronic Data Systems, Hewlett-Packard Enterprise Services, Alabama Department of Corrections -TransUnion, Intelenet Global Services

Both of those listings involved an insider breach on the part of the outsourcing companies with those being EDS/HP and Intelenet respectively. Both of these companies with business process outsourcing and serve Fortune 500 clients.

Government Sector Pairings

Pairing #16: U.S. Department of Energy 2006 Breach – U.S. Department of Agriculture

This pairing consists of two nationwide organizations whose own employee records have been breached. The breaches were announced with less than a 20 days difference.

Pairing #17: U.S. Department of Defense - Oregon Department of Revenue

In this pairing the nationwide Department of Defense was initially matched with three state level organizations that were also breached by the same type of attack in the same year. Those were namely the Georgia Technology Authority, Nebraska Treasurer's Office and Oregon Department of Revenue. By means of random selection the latter of the three was chosen as the paired match.

Pairing #18: U.S. Department of Veterans Affairs via contractor Unisys Corporation - U.S. Department of Veteran Affairs

The U.S. Department of Veteran Affairs has been breached twice due to an insider threat both in 2006 and 2007. In the former case though the employee in question was an external hire belonging to the Unisys Corporation that has a FIRST member SOC in place.

Pairing #19: U.S. Department of Energy 2013 Breach - Administrative Office of the Courts, Washington

The listing concerning the U.S Department of Energy 2013 Breach was initially classified as of an unknown cause. According to a public report of the department though, it can be safely be classified as a successful hacking attempt (U.S. Department of Energy et al., 2013). It was paired with a same year breach of a state level organization.

Pairing #20: Department of Homeland Security – Harris County

Both of those 2013 successful hacking breaches involved records pertaining to the employees of their respective organizations. Of course the pairing strategy is also adhered to since a nationwide organization is compared to county level one.

Pairing #21: State of Indiana Official Website - Vermont Agency of Human Services

The initial search of the dataset produced three state level organizations that could be possible matches. Out of them however only the Vermont state has a lower population than Indiana and was therefore chosen as a match.

Pairing #22: State of Rhode Island Website – City of Lubbock

Two city level organizations were found to match this state level one. Those were the cities of Lubbock and Wickliffe. By random selection the former was selected as the matching pair.

Retail – Merchant Industries

Pairing #23: Polo Ralph Lauren, HSBC - DSW Shoe Warehouse, Retail Ventures

Both of the listings contained in this pairing involved the theft of credit card data. Moreover, they occurred in the same year. The credit cards involved in the first breach were exclusively issued by HSBC and their use monitored and protected by the company's SOC.

Other Industries

Pairing #24: AT&T 2009 Breach – Sprint

This pairing consists of two direct competitors suffering from the same breach type at the same year. Nonetheless, it can be considered unique since the amount of records breached in the Sprint listing has been calculated based on an estimation. The reason behind this is the fact that no other telecommunication companies of size similar to AT&T could be found in the sample.

According to Matt Sullivan a Sprint spokesman at the time of breach less than 1% of the company's customer base had their records stolen (Krebs, 2009). The company's customer base at the time of breach was 49.3 million (Wortham, 2009). To calculate the amount of records breached the very conservative assumption was made that only 0.1% of the customer base's records were breached.

Pairing #25: Symantec - Electronic Data Systems (pre HP)

The reader should not be confused with finding Electronic Data Systems (EDS) on the non SOC side of the pairing contrary to pairing number 15. EDS has been acquired by Hewlett-Packard (who has a FIRST SOC in place) in 2008 and was rebranded as HP Enterprise Services. This listing comes from 2007.

Dropped Listings

Unfortunately some of the dataset's listings could not be effectively matched. Two of them pertain to AT&T and two of them to Adobe. The underlying reason is that there is a below par representation of IT and telecommunication companies in the known breached records dataset. Therefore matches adhering to the criteria specified previously could either not be found or resulted in pairings involving asymptotically similar organizations that were also advocating heavily for the SOC side. In the interest of soundness of results the following listings were dropped:

- Dropped Listing #1: Adobe, PR Newswire, National White Collar Crime Center 2013 Data Breach
- Dropped Listing #2: Adobe, Washington Administrative Office of the Courts 2013 Data Breach
- Dropped Listing #3: AT&T via vendor that operates an order processing computer 2006 Data Breach
- Dropped Listing #4: AT&T 2014 Data Breach