



Nova Southeastern University
NSUWorks

CEC Theses and Dissertations

College of Engineering and Computing

2016


An Analysis of the Relationship between Security Information Technology Enhancements and Computer Security Breaches and Incidents

Linda Betz

Nova Southeastern University, lindanbetz@gmail.com

This document is a product of extensive research conducted at the Nova Southeastern University [College of Engineering and Computing](#). For more information on research and degree programs at the NSU College of Engineering and Computing, please click [here](#).

Follow this and additional works at: http://nsuworks.nova.edu/gscis_etd

 Part of the [Databases and Information Systems Commons](#), [Finance and Financial Management Commons](#), [Information Security Commons](#), [Management Information Systems Commons](#), [Portfolio and Security Analysis Commons](#), and the [Technology and Innovation Commons](#)

Share Feedback About This Item

NSUWorks Citation

Linda Betz. 2016. *An Analysis of the Relationship between Security Information Technology Enhancements and Computer Security Breaches and Incidents*. Doctoral dissertation. Nova Southeastern University. Retrieved from NSUWorks, College of Engineering and Computing. (960)
http://nsuworks.nova.edu/gscis_etd/960.

This Dissertation is brought to you by the College of Engineering and Computing at NSUWorks. It has been accepted for inclusion in CEC Theses and Dissertations by an authorized administrator of NSUWorks. For more information, please contact nsuworks@nova.edu.

An Analysis of the Relationship between Security Information Technology
Enhancements and Computer Security Breaches and Incidents

by

Linda Betz

A dissertation submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy
in
Information Systems

Graduate School College of Engineering and Computing
Nova Southeastern University

April 2016

We hereby certify that this dissertation, submitted by Linda Betz, conforms to acceptable standards and is fully adequate in scope and quality to fulfill the dissertation requirements for the degree of Doctor of Philosophy.

Ling Wang, Ph.D.
Chairperson of Dissertation Committee

Date

Faith Heikkila, Ph.D.
Dissertation Committee Member

Date

Gertrude W. Abramson, Ed.D.
Dissertation Committee Member

Date

Approved:

Ronald J. Chenail, Ph.D.
Interim Dean, College of Engineering and Computing

Date

College of Engineering and Computing

Nova Southeastern University

2016

An Abstract of a Dissertation Submitted to Nova Southeastern University
in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy

An Analysis of the Relationship between Security Information Technology Enhancements and Computer Security Breaches and Incidents

by
Linda N. Betz

April 2016

Financial services institutions maintain large amounts of data that include both intellectual property and personally identifiable information for employees and customers. Due to the potential damage to individuals, government regulators hold institutions accountable for ensuring that personal data are protected and require reporting of data security breaches. No company wants a data breach, but finding a security incident or breach early in the attack cycle may decrease the damage or data loss a company experiences. In multiple high profile data breaches reported in major news stories over the past few years, there is a pattern of the adversary being inside the company's network for months, and often law enforcement is the first to inform the company of the breach.

The problem that was investigated in this case study was whether new information technology (IT) utilized by Fortune 500 financial services companies led to the changes in data security incidents and breaches. The goal of this dissertation is to gain a deeper understanding on how IT can increase awareness of a security incident or breach, and can also decrease security incidents and breaches. This dissertation also explores how threat information sharing increases awareness and decreases information security incidents and breaches. The objective of the study was to understand how changes in IT can influence an increase or decrease in data security breaches.

This investigation was a case study of nine Fortune 500 financial services companies to understand what types of IT increase or decrease detection of security incidents and breaches. An increase in detecting and stopping a security incident or breach may have positive effects on the security of an enterprise. The longer a hacker has access to IT systems, the more entrenched they become and the more time the hacker has to locate data with high value. Time is of the essence to detect a compromise and react. The results of the case study showed that Fortune 500 companies utilized new IT that allowed them to improve their visibility of security incidents and breaches from months and years to hours and days.

Acknowledgements

I would like to thank Professor Ling Wang for being on my dissertation committee, and taking over as my dissertation chair when Professor Marlyn Littman retired. I am deeply grateful that Professor Wang directed me in a clear path to finish my dissertation. I appreciate the guidance, efficiency, and improvements she has contributed to this dissertation. I was very lucky that Professor Littman asked Dr. Heikkila to be part of the dissertation committee. Dr. Heikkila's provided me detailed feedback that improved this dissertation. I appreciate Professor Gertrude Abramson's willingness to join the dissertation committee midstream.

I would like to acknowledge the participants in the study. I am grateful that they were willing to share their precious time and insights with me.

I would also like to thank Dr. Sharon Bear, my editor.

I am very appreciative to both IBM and Travelers. I started this journey while at IBM, and received support and encouragement from my management team. Travelers has been exceptionally supportive, and I appreciate the support and encouragement of my current management team, especially Steve Paquette and Madelyn Lankton. I have been surrounded by exceptional colleagues at IBM and Travelers, who have increased my knowledge in information security, and who I have been privileged to work with.

I have had the great opportunity to interact with many impressive individuals that have had attained their PhD. I had the opportunity to be on the board of Women in Engineering ProActive Network (WEPAN), I am currently on the board of trustees for the University of St. Joseph, my sister Dr. Katherine Betz, and Dr. Terry Escamilla who has been a longtime colleague. I have appreciated being surrounded by folks I respect that have modeled the way for me.

I appreciate my family and friends support and encouragement, and I am grateful that my mother instilled a belief and confidence in me.

Table of Contents

Abstract ii

List of Tables v

1. Introduction 1

Problem Statement 8
Dissertation Goal 11
Research Questions 13
Relevance and Significance 13
Barriers and Issues 19
Assumptions, Limitations, and Delimitations 19
Definition of Terms 20
Summary 28

2. Review of the Literature 28

Financial Services Security Regulations 29
Health Insurance Portability and Accountability Act of 1996 (HIPAA) 30
Industry Data on Security Threats and Breaches 31
Business Enablement IT 42
Security Analytics IT 49
Enhanced Security Control IT 50
Security Information-sharing Forums 53
Best Practices 55
Summary 65

3. Methodology 67

Research Methods 67
Research Design 68
 Research Questions 68
 Propositions 69
 Unit of Analysis 71
 Linking Data to Propositions 71
 Findings Interpretation 71
Reliability 72
Validity 72
Format of Presentation Results 73
Resources Required 73
Summary 74

4. Results 76

Review of the Methodology 76
Data Analysis 77
Summary of Results 92

5. Conclusions, Implications, Recommendations, and Summary 94

Conclusions 94

Strengths 102

Weaknesses 102

Limitations 103

Implications and Recommendations 103

Summary of the Study 1062

Appendices

A. List of Acronyms 112

B. Survey Instrument 115

C. Interview Responses 117

References 137

List of Tables

Table

1. Propositions 69
2. Summary of Results 90

Chapter 1

Introduction

Background

According to the Financial Stability Oversight Council, which consists of the US Treasury, the Federal Reserve System, and multiple federal financial services government regulators, a key threat and vulnerability of the financial services sector is cyber attacks (FSOC, 2015).. Data security breaches are a concern for financial services companies due to the possible impact on customer service, lawsuits, loss of reputation, and regulatory penalties (Andoh-Baidoo, Amoako-Gyanpah, & Osei-Bryson, 2010). Nevertheless, having a security policy in place does not prevent or reduce such breaches. Wiant (2005), Doherty and Fulford (2005), and Heikkila (2009) explored the relationship between security policies and data security breaches, and the findings of all three investigations demonstrated that there was no statistically significant relationship between having a security policy and realizing a reduction in data security breaches. This dissertation was a case study to explore the relationship between information technology (IT) and data security breaches and incidents, focused on the Fortune 500 financial services sector.

Data breaches occur in many industry sectors, which underscores how rampant a problem data security breaches are. The Privacy Rights Clearinghouse (2015) website provides a list of publicly disclosed data breaches starting from 2005, demonstrating how data breaches affect many sectors, including education, healthcare, and government. Universities have identified breaches; for example, the University of Washington in November 2013 reported the loss of 90,000 records when a hacker accessed their system.

Insurance company breaches include Blue Cross of California, which reported that, in November 2013, it exposed 25,400 doctors' social security numbers (Privacy Rights Clearinghouse, 2015). Government agencies have experienced data breaches, including the New York City Police Department, which reported the loss of 30 passwords from police officers when a former police detective paid a hacker to steal their passwords (Privacy Rights Clearinghouse, 2015). In 2013, Target reported a data breach that affected 70 million customers, in which the hackers gained access to credit and debit card information (Privacy Rights Clearinghouse, 2015). Anthem reported a major data breach in 2015, exposing social security numbers and health information of customers. The Privacy Rights Clearinghouse reported that the actual attack may have started 10 months prior to the breach identification. Some other noteworthy breaches in 2015 included the breach of CareFirst BlueCross BlueShield's 1.1 million records, Premera's 11 million records, Excellus BlueCross BlueShield's 10 million records, Experian's 15 million records, and ScottTrade's 4.5 million records as well as the IRS breach of 700,000 individuals' records and the U.S. Office of Personal Management's breach of 21.5 million records (Privacy Rights Clearinghouse, 2015). Data breaches span Fortune 500 financial services and many other public and private sector organizations.

The Ponemon Institute (2014), with the financial support of IBM Corporation, conducted an investigation that provided information on the cost of security data breaches. Specifically, the Ponemon Institute examined the cost of data breaches among 314 companies across 10 countries; the average size cost of a data breach per record exposed was \$145. In 30% of the data breaches, human error was the cause of the breach. Malicious or criminal attacks represented 42% of data breaches, and system glitches that

included both IT and business process failures contributed to 29% of the data breaches (Ponemon Institute, 2014). Regulations make it difficult for companies to hide data breaches, and investments in information security are not solving the data breach challenge. Caldwell (2014) pointed out that spending to improve cyber defenses, as related to the overall IT budget has increased, but the number and impact of breaches also are increasing.

In 2011, the U.S. Securities and Exchange Commission (U.S. SEC; 2011) advised publicly held companies registered with the SEC to disclose, in the Management's Discussion and Analysis portion of their SEC filing, details of a cyber attack that could disrupt operations as a consequence of additional remediation costs, increased cybersecurity protection costs, lost revenue, litigation, or reputational damage (Romeo & Parrino, 2012). In 2015, the U.S. SEC expanded their guidance around cyber security. The 2015 guidance urged financial services companies to create a strategy to prevent, detect, and respond to cyber security threats. The guidance also suggested that financial services companies conduct assessments of information security data protection, security controls, and vulnerability detection systems. Companies are not required to disclose the details of a cyber attack if the disclosure could compromise the registrant's security (Romeo & Parrino, 2012; U.S. SEC, 2011). Fortune 500 financial services companies are regulated to report data breaches that result from cyber attacks.

Nakashima and Douglas (2013) reported that several banks disclosed security incidents, per the SEC guidance regarding the distributed denial of service (DDoS) attacks and hacking of the U.S. banking community. The U.S. government attributed the DDoS attacks to the Iranian government in retaliation for sanctions imposed in response

to Iran's nuclear program. Banks that reported the security attacks to the SEC in their annual reports include Bank of America, Wells Fargo, and JPMorgan Chase (Nakashima & Douglas, 2013). Nakashima and Douglas pointed out that the executive order on cybersecurity that President Obama signed on February 12, 2013, is aimed at helping companies that are critical to the nation to provide stronger network security.

Security regulations and best practices influence the creation of security products. Symantec (2010) provided a list of regulations and industry best practices for companies to utilize when developing or enhancing their security strategy or investing in security products. McAfee (2013a) showed how their products could help companies to meet a wide variety of security regulations. Further, Cisco (2014a) offers security solutions that span firewalls, intrusion prevention systems, and spam filters to improve information security technology defenses. Many products exist for companies to improve their information security technology.

A variety of regulations require a financial services company to report a data security breach. The regulations include state security breach notification laws and federal laws, such as the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act (GLBA; Stevens, 2012). The Financial Industry Regulatory Authority (2012) released a regulatory notice in 2012, recommending that financial firms review their procedures for protecting customer information due to increased fraud stemming from malware that compromised customer computers.

The Office of the Comptroller of the Currency (OCC; n.d.) regulates and supervises national banks and federal savings associations. The OCC requires the Federal Financial Institutions Examination Council (FFIEC) to produce IT handbooks to be used by the

OCC to examine the information security of banks and savings associations (OCC, n.d.). Further, many financial services companies issue or utilize credit cards and can be subject to the Payment Card Industry Data Security Standard (PCI-DSS; PCI Security Standards Council [SSC], 2006; Stevens, 2012). In 2014, the National Institute of Standards and Technology (NIST; 2014b) released a cyber security framework that is mandatory for government-selected critical infrastructure and a guideline for other companies. Financial services institutions may be subject to multiple regulations around information security and breach notification.

Gartner defines security information and event management (SIEM) as technology that supports threat detection and incident response, using real-time security event data to correlate and analyze events (Burnham, 2013). SIEM technology provides security analytics that allow for mining of log data to piece together a picture of a malicious security event (Lozito, 2011; Oltsik, 2013). Gartner publishes their view of the top products in a particular area and rates products by their ability to deliver function and an articulate product roadmap, and their choice of superior products is called the magic quadrant (Burnham, 2013). For SIEM technology, IBM Q1 labs, HP ArcSight, McAfee Nitro, Splunk, and LogRhythm were named to the 2013 Gartner's magic quadrant (Burnham, 2013).

According to Lozito (2011), SIEM has emerged as a security tool to allow deeper analysis of both real-time and historical events. SIEM enables companies to perform security analytics to search for anomalies in log data, providing the capability to locate possible compromises (Chickowski, 2011). Use of SIEM technology could lead

institutions to discover security incidents of which they were previously unaware (Gabriel, Hoppe, Pastwa, & Sowa, 2009).

Nevertheless, as companies change their computing models, new security risks can emerge. For example, cloud technologies are an option that companies can utilize to react quickly to evolving business requirements, rather than taking the time to develop custom solutions within the company (Sadiku, Musa, & Momoh, 2014). Many different cloud offerings are available, including Infrastructure as a Service (IaaS), Software as a Service (SaaS) and Platform as a Service (PaaS; Columbus, 2013; Sadiku et al., 2014). IaaS provides storage, processing, and network services from the Internet. An example of an IaaS is Amazon's Elastic Compute Cloud (Sadiku et al., 2014). PaaS builds upon the IaaS capabilities by adding application programming interfaces. Google AppEngine and Microsoft Azure are two examples of PaaS cloud technology (Sadiku et al., 2014). A SaaS is directly consumable by a user, not requiring the company's IT organization to provide customization of the cloud service. An example of a SaaS is Salesforce (Sadiku et al., 2014).

New IT can create information security implications. If the cloud offering is hosted external to the company, the level of security responsibility changes, depending on the service offering that is chosen. In an IaaS service offering, the customer is provided storage and processing capabilities (Sadiku et al., 2014). In a SaaS model, the cloud provider provides all of the security components (Bejtlich, Steven, & Peterson, 2011; Cadregari & Cutaia, 2011; Dai Zovi, 2011; Grobauer, Walloschek, & Stocker, 2011; Johnson & Pfleeger, 2011; Lesk, 2012; Nguyen, 2011; Ryan, 2011; Stevens, 2011; Weis & Alves-Foss, 2011).

Kothari (2013) explained that cloud technologies may provide companies with a faster method to deploy applications but include risks that should be considered. Kothari highlighted that the primary cloud security risk is protecting regulated data, specifically, data held by banks and insurance companies. Some examples of security risks related to cloud technology are data protection, data disposal, physical controls, access controls, logical controls, and reporting obligations (Cadregari & Cutaia, 2011). Ginovsky (2013) urged banks to consider several risks when contemplating the use of outsourced cloud technologies. These risks include vendor health, data segregation, data security, data backup, cloud providers' contractual obligations, eDiscovery, and an exit plan (Ginovsky, 2013). Therefore, as financial services institutions utilize new IT, such as cloud technologies, consideration should be given to security, data breach, and regulatory risks (Kothari, 2013).

The FFIEC has updated their information on managed security service providers to include guidance on using cloud services, which outlines several additional security and risk considerations for financial companies to comply with (FFIEC, 2012b). The FFIEC requires regulated financial institutions to protect data in transit, secure data at rest, comply with regulatory requirements, comply with offshore data privacy laws, and avoid sharing authentication credentials (FFIEC, 2012b). Fortune 500 financial services companies need to consider new regulatory guidance.

The public cloud is gaining greater adoption by businesses (Columbus, 2013). Global spending on cloud computing is expected to grow at a compound annual growth rate of 17.7% between 2011 and 2016 (Columbus, 2013). Banks are increasing their investments in public cloud services. In a survey of 115 large banks by

PricewaterhouseCooper (PwC), 71% of bank executives plan to invest more in cloud computing, which is an increase of four times over the previous year (Crosman, 2013). As Fortune 500 financial services companies host more data in public clouds, new information security challenges arise. Results from a survey conducted by PwC (2015) on the state of information security showed that there was a 38% increase in the security incidents detected, while information security budgets grew by 24% in 2015 over 2014.

Problem Statement

Data security breaches can have a financial impact on U.S. publicly traded companies, including Fortune 500 financial services companies (Goel & Shawky, 2009). Financial implications include government fines, expenses related to lawsuits, costs of notification to individuals with lost personal information (PI), costs to provide identity theft protection, and loss of intellectual property that results in a decreased competitive edge or loss of market value (Goel & Shawky, 2009). Goel and Shawky analyzed U.S. publicly traded firms with breaches that were made public between 2004 and 2008 and reported that there was a negative effect on the company market value the day of the breach, as well as a highly significant negative impact on the company stock price on the day following the incident. On average, U.S. publicly traded companies experienced a 1% loss of market value over a period of five days from the announcement of a security data breach (Goel & Shawky, 2009). In addition to the cost of the data breach, there are longer term implications. Afroz, Islam, Santell, Chapin, and Greenstadt (2013) found, in a survey of 600 participants, analyzing three data breaches of Apple, Sony, and Facebook, that consumers are less likely to purchase products from companies that experience a data breach.

Security breaches also may have an impact on consumers. Javelin (2013) identified an increase of one million victims of identity fraud incidents in 2013. One in four breach notification recipients become a victim of identity fraud (Javelin, 2013).

Verizon (2013) has been publishing an annual report on data breaches since 2004. In 2012, they analyzed 855 incidents, resulting in 175 million compromised records. The companies in the report represented 36 countries, including the United States, and company size spanned from fewer than 10 employees to over 100,000. The companies comprised multiple industries, including financial services, retail, accommodations, food service, healthcare, and IT. According to Verizon, in most of the breaches, there was a delay between the data breach and the discovery. They reported that, in 54% of the data breaches, it took from one to 12 months from the time that the system was initially compromised to the discovery of the data breach. Further, third parties discovered most of the breaches; for example, the Federal Bureau of Investigation (FBI) discovered 59% of the data breaches, and payment card processors, such as PayChex and Fiserv, identified fraud in 26% of the breaches (Verizon, 2013).

The Verizon (2013) study demonstrated that companies may not realize that they have had a data breach for many months or even years. The FBI confirmed that they were investigating the reported breaches experienced by Dun and Bradstreet, Kroll Background America, and LexisNexis (Finkle, 2013); further, KrebsOnSecurity reported that the LexisNexis breach likely occurred five months prior to LexisNexis's being aware of the security breach (Finkle, 2013; Krebs, 2013).

Financial institutions continue to have data breaches, as evidenced by the number of reported breaches (Verizon, 2013). In March 2013, TD Bank lost two unencrypted

backup tapes that contained customer data (Privacy Rights Clearinghouse, 2015). In April 2013, Prudential Insurance sent an email that contained customers' data to the wrong recipient (Privacy Rights Clearinghouse, 2015). In November 2012, Nationwide lost one million customer records due to a cyber attack (Privacy Rights Clearinghouse, 2015). In September 2012, Lincoln Financial lost 4,657 customer records, also due to a cyber attack (Privacy Rights Clearinghouse, 2015). In 2014, hackers were able to gain access to PI from 76 million J. P. Morgan Chase account holders (Privacy Rights Clearinghouse, 2015).

These examples demonstrate weaknesses that may exist from security incidents and breaches caused by people, processes, and technology. Heikkila (2009) examined whether the existence of a security policy had a relationship to the number of security breaches a company experienced. In her research, Heikkila hypothesized that IT, specifically, virus detection, increased the ability to detect a security incident or breach. As IT security tools have expanded beyond merely virus detection technology in relation to the implications to incidents and breaches, this research analyzed which IT increase or decrease security incidents and breaches, and whether the enterprise believes that the technology strengthened or weakened their overall enterprise security. The problem investigated in this case study was whether new IT utilized by Fortune 500 financial services companies led to the changes in data security incidents and breaches. This dissertation also explored how threat information sharing increases awareness and decreases information security incidents and breaches.

Dissertation Goal

The goal of this dissertation is to gain a deeper understanding on how information technology can increase awareness of a security incident or breach, and can also decrease security incidents and breaches. This dissertation also explores how threat information sharing increases awareness and decreases information security incidents and breaches. Heikkila (2009) identified the need for further research to understand whether greater levels of IT sophistication can increase an institution's ability to detect a data security breach. The intent of this investigation was to determine the role of IT with respect to increasing or decreasing data security breaches. Incidents could increase or decrease as a result of better detection, improved prevention, remediating risks, improved threat intelligence, or changing IT compute models. More specifically, the concern was whether different types of IT lead to an increase or decrease awareness in the number of security incidents and breaches that have occurred.

This case study examined Fortune 500 financial services companies, and what type of IT increases or decreases security data breaches or incidents. The Financial Services Information Sharing and Analysis Center (FS-ISAC) is a leading cyber threat intelligence institution for financial services. FS-ISAC members span banks, credit unions, insurance companies, and credit card companies. Financial services within this investigation included companies that fall under the scope of FS-ISAC membership. Increases in detecting security incidents and breaches include the company's awareness of an incident of which, prior to the implementation of the IT solution, the company could have been unaware.

Specifically, several categories of IT were explored in relation to security incidents. The categories included IT that (a) provides enhanced security protections, such as data loss prevention (DLP), Internet content filtering, and limiting administrative rights; (b) provides enhanced security correlation and data analysis, for example, log consolidation, log monitoring, and SIEM; (c) enhances business capabilities, such as cloud and mobile computing; and (d) threat intelligence services, for example, FS-ISAC or InfraGard Members Alliance (InfraGard, 2015).

The number of security incidents and breaches may increase or decrease for many reasons. Reasons that security incidents may increase include (a) the sophistication of the hackers improves (Strohm, 2013); (b) companies improve their information security detection and are able to find compromised systems of which they previously would have been unaware (EMC², 2013); and (c) companies are using new productivity tools, such as mobility and cloud services, that provide a more complex environment and more attack points for hackers (Seltzer, 2012). The sophistication of hackers may be the result of the underground economy's enabling hackers to buy hacking tools or compromised servers. Gonsalves (2013) reported that a 1,000-computer botnet, i.e., a type of malware that a hacker uses to control an infected computer, is currently priced at \$120. Reasons that security incidents may decrease include: (a) companies are using new security technology that prevents the compromise of systems (Ohlhorst, 2013); and (b) companies share security threat information through organizations such as FS-ISAC (2013a), utilizing security intelligence data to block attacks. The U.S. government provides free information on information security threats through the Cyber Emergency Response Team (CERT). The U.S. CERT (2014) website provides information on current security

issues, vulnerabilities, and exploits. Changing threats, IT, and security intelligence can affect data security incidents and breaches.

Research Questions

The following research questions were addressed:

RQ 1: What type of information security products result in an increased detection of security incidents and breaches?

RQ 2: What types of security information technology result in a decrease of security incidents and breaches?

RQ 3: How have new technologies, for example, cloud and mobile technologies, resulted in an increase or decrease in data security incidents and breaches, and has the technology strengthened or weakened enterprise security?

RQ 4: To what extent can participation in threat-information sharing groups, or threat intelligence information sharing, increase awareness of security incidents and breaches?

Relevance and Significance

Over the past decade, there have been increased government guidance and regulations for financial services institutions to report breaches (Romeo & Parrino, 2012; U.S. SEC, 2011). Importantly, new regulations related to the Presidential Executive Order on Cybersecurity (White House, 2013) have been released (NIST, 2014b). The NIST cyber guideline was created to help organizations that are part of the U.S. critical infrastructure to better protect information from a cyber attack (NIST, 2014a). As of 2015, the NIST cybersecurity framework is voluntary for noncritical infrastructure and mandatory for government defined critical infrastructure. The goal of the NIST cybersecurity

framework is to provide best practices for improving security and resiliency of U.S. companies (NIST, 2014a). The guideline is broken into five areas: identify, protect, detect, respond, and recover (NIST, 2014b).

Current legislation, such as HIPAA and GLBA, require reporting of data breaches. As a consequence, financial services companies that hold Personally Identifiable Information (PII) are subject to data breach regulations and are motivated to decrease data breaches (van Kessel & Allan, 2013). Moreover, corporate boards of directors also are concerned about the impact of a security breach on the company (Reeves & Stark, 2011; Savitz, 2011).

Data breaches occur not only from external forces; some are perpetrated by end users (Verizon, 2013). Two examples of user errors cited by the Privacy Rights Clearinghouse (2015) are; (a) an employee of Mass Mutual who sent an unencrypted email that contained the name and social security number of a customer to a third party by mistake in 2013; and (b) an employee at Citibank who, in 2013, misconfigured a website, allowing people to see other users' account information. In some cases, technology can help to reduce or prevent human error.

Miyamoto (2013) identified people as the weakest link in information security. People can misjudge a situation that leads to malware infections or data leakage, for example, clicking on a malicious attachment in an email (Miyamoto, 2013). Lack of security training, organizational culture, not understanding the risk, being more motivated to get the work accomplished than complying with security controls, and making an unintentional error are some of the reasons that end users cause security issues (Miyamoto, 2013).

Many security products exist to address the challenge of human error, two of which are Internet content filtering and DLP. An example of a product that provides Internet content filtering is Cisco's (2014b) Adaptive Security Appliance (ASA) Content and Security Control. This provides an anti-virus solution to scan any files downloaded, eliminate spam to reduce the chance of people's responding to phishing attempts, and allow organizations to limit what sites employees visit, including sites that are malicious or compromised (Cisco, 2014b).

CA Technologies (2015) provides data protection solutions, which allow an organization to set up rules to look for data strings or document tags and prevent data from leaving the company. For example, if a company does not want social security numbers to be emailed out of the company, data protection allows a company to block any emails that contain social security numbers (CA Technologies, 2015).

In 40% of the incidents that Verizon (2013) investigated, the attacker took a day or more to exfiltrate data from a victim's IT systems. Of note is that, in 54% of the data breaches, it took between one and 12 months from the time that the system was initially compromised to the discovery of the data breach (Verizon, 2013). Companies may be unaware that they have been compromised and that a data breach has occurred (Verizon, 2013).

The Target data breach gained government attention. In a Senate majority staff report led by Chairman Jay Rockefeller on March 26, 2014 (U.S. Senate, 2014), the details of the Target data breach are outlined, including that the financial and personal records of 110 million Target customers were compromised and that the records were routed to a Russian server. The attack started through a third-party HVAC provider compromised

machine that had access to Target's network. Target had multiple layers of security that noticed the malware and provided alerts, but the alert was not raised to a sufficient level to take action. . Specifically, the FireEye malware intrusion detection system and Symantec software both recognized and alerted on the malware intrusion. However, the hackers were able to take control and loaded malicious code onto the point-of-sales systems, which provided the avenue to syphon off customer data.

The malware was installed between November 15, 2013, and November 30, 2013. Target became aware of the breach on December 12, 2013, when the Department of Justice contacted Target (U.S. Senate, 2014). The Senate majority staff report indicated that additional IT might have prevented the breach. Specifically, Target did not have Internet content filtering capabilities or a whitelisting process for file transfer protocol data transfers, which would limit the destinations of communication flow. In the timeline outlined in the report, it was a month from the first breach of the Target system to when the Department of Justice contacted Target.

It may take a large company (companies with over 1,000 employees) months or even years to detect a data breach (Goel & Shawky, 2009; Verizon, 2013). Companies with the ability to quickly detect a security incident or breach create an opportunity to reduce the amount of data loss from a compromised system (Verizon, 2013). The ability to catch the attacker in the process of compromising a system may even stop a data breach (Verizon, 2013).

In addition, reducing the window between the initial compromise and discovery could avert a data breach (Chickowski, 2013). In the example of the Target breach, Target missed multiple opportunities to respond to security alerts from the FireEye and

Symantec security products (Chickowski, 2013). The longer it takes to respond to an attacker, the more firmly rooted the attacker can become within the IT infrastructure (Chickowski, 2013). If a company is able to detect a system compromise by an insider or hacker in one day, the negative long-term effects may be more limited than they would be if the same system compromise took a year to be detected (Verizon, 2013).

A class of solutions that could help identify security threats are endpoint security products that provide monitoring of endpoints and create alerts of suspicious activity. An example is McAfee Complete Endpoint Protection—Enterprise (McAfee, 2014a). Utilizing McAfee's ePolicy Orchestrator console, an administrator could be alerted to suspect activity or policy non-compliance. To reduce the chance of endpoint infections, a company could install products that detect malicious code that comes in from the Internet. Additionally, FireEye (2013b) provides products that have the ability to detect whether files that enter a system are malware and block the file or alert the administrator. With both of these products, additional alerting provides a company the chance of discovering and responding to malicious activity.

Roos (2013) found in a study of 248 security professionals that, even with the benefits of reducing the amount of time to detect a hacker who has gained access to a company's IT systems, only 24% of the respondents used automated technologies, such as monitoring for privilege escalation, suspicious data access, and file access changes, to detect a security data breach. In addition, an increase in data security incidents and breaches may not be due to carelessness or inadequate security. Rather, it may be an indication of increased security sophistication to detect the event (Chickowski, 2013).

Roos explained that, in 36% of large enterprises, automation exists to detect access control changes, compared to 28% in companies overall.

There are multiple products on the market that allow companies to monitor data file activities (Imperva, 2015, Tripwire, 2015; Varonis, 2013). Products like Varonis provide the capability to monitor access to sensitive files. Varonis DatAdvantage for Windows contains technology that allows an organization to identify sensitive data, monitor who has access to the data, and be alerted when data are accessed. The product allows an administrator to receive alerts for anomalous behaviors and privileged access escalation (Varonis, 2013).

Even with sophisticated IT security however, companies can fail to react to alerts (Vijayan, 2014a). Vijayan identified scenarios where technology may not be adequate to stop malware. For instance, companies may install a security product but lack a subject matter expert, or an organization may install a technology with product defaults, creating too many alerts to review and follow up on. If there are too many false positive alerts, a staff can get overwhelmed and miss a real attack (Vijayan, 2014a). In the case of the Target breach, Vijayan pointed out that security alerts occurred, but the Target security staff did not take appropriate action.

This dissertation research expands on knowledge that pertains to how information security technologies increase or decrease the number of security incidents and breaches detected and whether having access to threat intelligence drives greater awareness, leading to more or fewer security incidents. An increase in security incidents could be the result of better detection, improving the overall enterprise security of the company.

The focus of the research was a subset of financial services Fortune 500 companies. Financial services are a top target for hackers due to the financial gain that can be achieved from a data breach (InformationWeek, 2012). IT industry papers and articles describe technology gaps that could detect or prevent data security breaches (Chickowski, 2013; IBM, 2013; van Kessel & Allan, 2013; Verizon, 2013). This research focused on providing information pertaining to the utilization of IT security and whether the new IT security technology increased or decreased data security incidents and breaches in Fortune 500 financial services companies. The results provided details on how Fortune 500 financial services companies are applying IT security technology, and the results they are experiencing. .

Barriers and Issues

Companies are reluctant to respond to surveys on information and security breaches. This reluctance is demonstrated by the typically low response rate to security research surveys, unless there is an established relationship with the survey organizations. For example, Heikkila (2009) distributed a Web-based survey to 1,123 Information Legal Technology Association members and received 88 valid responses, a 7.83% valid response rate. Doherty and Fulford (2005) surveyed 2838 people with a 7.7% valid response rate. Wiant (2005) surveyed 2500 people with a 5.6% response rate. Finding willing participants are an integral part of information security research.

Assumptions, Limitations, and Delimitations

Ellis and Levy (2009) define an assumption to be what researchers take for granted. Assumptions of the this study included: (a) participants would be honest and not hold

back data when responding to interview questions; (b) participants held broad enough knowledge as leaders of their company to answer interview questions accurately; and (c) the author was not biased and would not perform incorrect pattern matching with the available data.

Delimitation refers to the factors, constructs, and/or variables intentionally left out of the study (Ellis & Levy, 2009). Delimitations can affect external validity or generalizability (Ellis & Levy, 2009). Delimitations of this study were (a) the study was focused only on Fortune 500 financial services companies, and generalization outside of this sector was limited; and (b) the sample size of nine security professionals in the Fortune 500 financial services sector may have affected generalizability.

Definition of Terms

Advanced Persistent Threat: A deliberately slow-moving cyber attack that is applied quietly to compromise information systems (Friedberg & Skopik, 2015).

Bot: A term short for robot. Criminals distribute malicious software that can turn a computer into a bot. When this occurs, a computer can perform automated tasks over the Internet without one's awareness (Microsoft, 2014a).

Botnet: Criminals use bots to infect large numbers of computers. These computers form a network, or a botnet. Criminals use botnets to send out spam email messages, spread viruses, attack computers and servers, and commit other kinds of fraud (Microsoft, 2014a).

Bring Your Own Device (BYOD): Mobile devices that are personally owned, not a corporate asset (NIST, 2013d).

Brute Force Password Attack: A method of accessing an obstructive device through attempting multiple combinations of numeric and/or alphanumeric passwords (NIST, 2013e).

Buffer Overflow: A condition where more input is placed into a buffer than the capacity allows, overwriting other information. Attackers exploit such a condition to crash a system or insert malicious code to gain access to the system (NIST, 2013e).

Consumer Financial Protection Bureau (CFPB): A federal agency tasked with ensuring that consumers get the information they need to make financial decisions based on clear, up-front pricing and risk visibility. The CFPB regulates unfair, deceptive, or abusive practices by financial institutions (CFPB, 2015).

Containerization: An isolated space on a mobile device that allows for separation, data protection for the company device, and privacy for personal data of the user (NIST, 2013d).

Crimeware: Tools that drive hackers' attacks and fuel the black market (e.g., bots, Trojan horses, spyware; Norton, 2014)

Cryptocurrency: A digital medium of exchange that uses encryption to secure the process involved in generating units and conducting transactions (WhatIs, 2016).

Cyber Attack: An attack, via cyberspace, that targets an enterprise's use of cyberspace for the purpose of disrupting, destroying, or maliciously controlling a computer environment/infrastructure; destroying the integrity of the data; or stealing controlled information (NIST, 2013e).

Data Breach: An organization's unauthorized or unintentional exposure, disclosure, or loss of sensitive PI, such as social security numbers; financial information, such as credit card numbers; date of birth; or mother's maiden name (NIST, 2010).

Data Security Breach: An organization's unauthorized or unintentional exposure, disclosure, or loss of sensitive PI, which can include PII, such as social security numbers; or financial information, such as credit card numbers (National Conference of State Legislators, 2013).

Data Security Incident: A violation or imminent threat of violation of a computer security policy, acceptable use policy, or standard security practice (NIST, 2012a); or an accessed occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information that the system processes, stores, or transmits (NIST, 2013e).

Data Loss Prevention (DLP): Products that safeguard intellectual property and ensure compliance by protecting sensitive data through policy rules and tagging documents to control the flow of data (Cisco 2014c; McAfee 2014b).

De-identification: A technique to find and remove sensitive information by replacing or encrypting the sensitive data (Rahmani, Amine, & Hamou, 2015).

Denial of Service (DoS): The prevention of authorized access to resources or the delaying of time-critical operations (NIST, 2013e).

Distributed Denial of Service (DDoS). An approach whereby the hacker attempts to make a service unavailable to its intended users by draining system or networking resources, using multiple attacking systems (Wang, Zheng, Wenjing, & Hou, 2014).

Federal Deposit Insurance Corporation (FDIC): Independent government agency that preserves and promotes public confidence in the U.S. financial system by insuring deposits in banks for at least \$250,000 and monitoring financial risks of banks (FDIC, 2015).

Federal Financial Institution Examination Council (FFIEC): Interagency body established in 1979 to provide uniform principles, standards, and reporting forms for federal examinations targeted at financial institutions (FFIEC, 2015a).

Federal Trade Commission (FTC): Independent government agency whose mission is to prevent business practices that are anti-competitive, deceptive, or unfair to consumers (FTC, 2015).

Federal Reserve System (FRS): The United States central bank. They set national monetary policy, supervise and regulate banks and other financial systems, and provide oversight to the U.S. payment system (Board of Governors of the Federal Reserve System, 2014).

Hacker: Unauthorized user who attempts to or gains access to an information system (NIST, 2013e).

Hypervisor: Software, firmware, or hardware that controls the flow of instructions between the guest operating system and the physical hardware (NIST, 2011).

Indicators of Compromise (IOCs): Pieces of forensic data, such as data found in system log entries or files, that identify potentially malicious activity on a system or network (TechTarget, 2015).

Information Sharing and Analysis Center (ISAC): Organizations segmented by industry segment, for example, communications, energy, emergency management,

financial services, healthcare, transportation, IT, maritime, nuclear, public transit, research and education, supply chain, and water. The purpose of an ISAC is to share security threat information within the industry sector and with the government; its goal to improve the security of the companies that participate in the ISAC (National Council of ISACs, 2013).

Intrusion Detection System: Hardware or software that gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions and misuse (NIST, 2013e).

Intrusion Prevention System: Systems that can detect and attempt to stop an intrusive activity, ideally before it reaches its target (NIST, 2013e).

Jailbreak: When a device is altered allowing the operating system to bypass security controls (Constantin, 2014).

Key Logger: A program designed to record which keys are pressed on a computer keyboard; used to obtain passwords or encryption keys for bypassing other security measures (NIST, 2013e).

Malicious Code: Software or firmware intended to perform an unauthorized process that will have an adverse impact on the confidentiality, integrity, or availability of an information system (NIST, 2013e).

Malware: Code targeted to infect a user's device. When successful, the hacker is able to control the user's device, which may lead to data loss or escalation in the hacker's privileges on the information system (Beuhring & Salous, 2014).

Mobile Application Management (MAM): Solutions that allow IT administrators to remotely install, update, remove, audit, and monitor enterprise applications on mobile devices (Eslahi, Var Naseri, Hashim, Tahir, & Saad, 2014).

Mobile Device: Smart phones, tablets, portable cartridge/disk-based, removable storage media (e.g., floppy disks, compact disks, USB flash drives, external hard drives, flash memory cards/drives that contain nonvolatile memory; NIST, 2013d, 2013e).

Mobile Device Management (MDM): System to remotely monitor the status of mobile devices to enforce security policies (Eslahi et al., 2014).

National Credit Union Administration: (NCUA). An independent federal agency that regulates, charters, and supervises federal credit unions. The NCUA insures millions of individual credit union account holders (NCUA, 2015).

Network Sniffing: A passive technique that monitors network communication, decodes protocols, and examines headers and payloads for information of interest. It is both a review technique and a target identification and analysis technique (NIST, 2013e).

Non-public Information: Information that is not publicly available that a consumer provides to a financial institution to obtain a product or service, for example, an account balance (OCC, 2011).

Office of the Comptroller of the Currency (OCC): Independent bureau in the U.S. Treasury that ensures that national banks and federal savings associations operate in a safe and sound manner, providing fair access to financial services, and comply with applicable laws and regulations (OCC, 2015).

Packet Sniffer: Software that observes and records network traffic (NIST, 2013e).

Protected Health Information (PHI): Individual identifiable health information transmitted or maintained in any form by a covered entity or business associate. PHI includes medical records, test results, and treatments. A covered entity includes healthcare providers, health plan providers, and healthcare clearing houses. A business associate is another company that processes data on behalf of the covered entity. ePHI is electronic protected health information (U.S. Department of Health and Human Services [HHS]; 2013b).

Personal Information: Information from individuals that can uniquely identify a specific person (NISTIR 8053, 2015).

Personal Identifiable Information (PII): Information that can be used to distinguish or trace an individual's identity, such as his or her name, social security number, or biometric records, alone, or when combined with other personal or identifying information that is linked to a specific individual, such as date and place of birth or mother's maiden name (NIST, 2013e).

Phishing: A digital form of social engineering that uses authentic-looking, but bogus, emails to request information from users, directs the user to a fake web site that requests information, or entices a user to open a malicious attachment (NIST, 2013e).

Privileged account: An information system account with approved authorizations of a privileged user (NIST, 2013e).

Privileged user: A user that is authorized to perform security relevant functions on a computer server that ordinary users are not authorized to perform (NIST, 2013e).

Ransomware: A type of malware that encrypts files and prevents the user from accessing data until the user pays a certain amount of money (ransom) to decrypt the files (Beuhring & Salous, 2014; Microsoft, 2014b).

Rootkit: A set of tools used by an attacker after gaining root-level access to a host to conceal the attacker's activities on the host and permit the attacker to maintain the access through covert means (NIST, 2013e).

Security and Exchange Commission (SEC): A federal agency whose mission is to protect investors; maintain fair, orderly, and efficient markets; and facilitate capital formation (U.S. SEC, 2013).

Security Event: Any observable security occurrence in a system network (NIST, 2012a).

Security Incident: A violation or imminent threat of violation of a computer security policy, acceptable use policy, or standard security practice (NIST, 2012a). These include an accessed occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information that the system processes, stores, or transmits (NIST, 2013e).

Security Information and Event Management (SIEM) Tool: Application that provides the ability to gather security data from information system components and present that data as actionable information via a single interface (NIST, 2013e).

Smartphone: Mobile phones with the ability to provide applications and multimedia communications (Longfei, Xiaojiang, & Xinwen, 2014).

SPAM: The abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages (Homeland Security, 2016).

Spyware: Software that is secretly or surreptitiously installed on an information system to gather information on individuals or organizations without their knowledge (NIST, 2013e).

Trojan Horse: A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program (NIST, 2013e).

Unauthorized User: A user who accesses a resource that he or she is not authorized to use (NIST, 2013e).

Virtualization: Hiding the discrepancy between the virtual and physical allocation of information technology resources (Jin, Seol, Huh, & Maeng, 2015).

Virtual Machine: A separate logical instance of resources for a user or application that in reality is shared physical hardware (Jin et al., 2015).

Worm: A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread malicious code (NIST, 2013e).

A complete list of acronyms is presented in Appendix A.

Summary

This chapter presents the research problem, specifically, how the use of IT affects the ability to protect or detect a security data incident or breach. The goal of this research was to provide more insight into how IT relates to the changes in security incidents and breaches. Prior research considered security policy (Doherty & Fulford, 2005; Heikkila, 2009; Wiant, 2005). Heikkila suggested further research to understand how the use of IT may affect data security breaches.

Chapter 2

Review of the Literature

This section presents the literature relevant to the security policies and regulations that are currently in effect with regard to the financial services industry, as well as industry data on security threats and breaches, business enablement IT, security products, and security threat-information sharing forums. The section concludes with literature on security best practices. The financial services sector includes insurance companies, which consists of institutions that could process and hold healthcare information for employees and customers; therefore, healthcare regulations are included. FS-ISAC (2013b) membership is open to financial institutions, insurance companies, and publicly held securities/brokerage firms. This research explored how IT and threat-intelligence sharing increase or decrease the identification of data security incidents and breaches.

Financial Services Security Regulations

Financial services are a highly regulated industry sector. Within the United States, the SEC and FTC have broad oversight over publicly traded financial services companies. This section presents the regulations as of 2015 that the financial services sector are required to meet and how government bodies are used to drive information security requirements for the financial services sector.

The FFIEC (2012a), established in 1979, is a U.S. government interagency regulatory body that consists of the Federal Reserve System (FRS), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of

the Comptroller of the Currency (OCC), and the Consumer Financial Protection Bureau (CFPB). The purpose of the FFIEC and its associated group of regulators is to provide federal supervision to financial institutions, including banks, bank holding companies, savings and loans, and credit unions (FFIEC, 2015a).

The FFIEC provides specific guidance regarding information security through the IT Examination Handbook (FFIEC, 2006), which states that regulated financial services sector companies should monitor networks and servers to detect activity for policy violations and anomalous behavior. If incidents are discovered, the FFIEC suggests that the regulated entity: (a) report the security incident to the appropriate groups, which could include law enforcement; (b) submit a suspicious activities report when critical information is stolen or critical systems are damaged; and (c) inform the industry ISAC of the details of the incident, as well as to inform other ISAC members to look for any common indicators of attack, such as an attacking IP address or a malware signature (FFIEC, 2006). In June 2013, the FFIEC started a working group to promote coordination between federal and state regulators to enhance communication among FFIEC member agencies regarding cybersecurity and protection of critical infrastructure (FFIEC, 2013). Financial services companies have multiple regulations around information security and data breach notification.

Health Insurance Portability and Accountability Act of 1996

The U.S. government Health Insurance Portability and Accountability Act of 1996 (HIPAA) was enacted to protect patient health data. HIPAA required doctors' offices and nursing companies to have an information security policy in place by April 20, 2005

(U.S. Department of HHS, 2013b). HIPAA also required healthcare providers, providers of health plans, and healthcare clearinghouses to implement access controls, audit controls, integrity controls, and transmission security on their IT systems (U.S. Department of HHS, 2013b). The HIPAA regulations not only drove changes in security policy but also required companies to consider IT security investments to meet the regulatory requirements.

The HIPAA security regulations affect not only doctors' offices and nursing homes, but also health insurance companies, companies that house data on institutions' health plans, and government programs that store health data. In addition, as part of the American Recovery and Reinvestment Act of 2009 (ARRA), HIPAA requirements were expanded to include having companies report, within 60 days of the discovery of the breach, any losses of unsecured PHI that affect individuals (Holloway & Fensholt, 2009). This expanded scope includes institutions that provide financial and administrative transactions (Holloway & Fensholt, 2009; U.S. Department of HHS, 2013a). Importantly, insurance companies are part of the financial services sector and may hold HIPAA-regulated data of customers or employees. ARRA, also known as the stimulus package, is a 407-page bill that provides government actions to improve the economy. The latest changes to HIPAA were driven through the ARRA bill (Track the Money, 2013).

Industry Data on Security Threats and Breaches

Security threats are the result of a malicious or criminal attack, a system glitch, or human factor (Ponemon Institute, 2014). The Ponemon Institute identified factors that can influence the cost of a data breach, including data that was lost by a third party or a

breach that involved stolen devices. The cost of a data breach can be reduced by a company's having a relatively strong security posture at the time of the incident, having an incident management plan, and having a chief information security officer (CISO) who has responsibility for enterprise data protection. Chapman, Leblanc, and Partington (2011) provided a base set of terminology of cyber attacks to better understand the threats from external hackers that could lead to data security incidents and breaches. For instance, a DoS attack overwhelms a computer's resources, making the computer system unable to respond to legitimate requests. Additionally, stack-based buffer overflow occurs when a poorly written application allows for insertion of code into a field that is executed, which allows a hacker to take unauthorized control (Chapman et al., 2011).

Other security threats include (a) phishing, which occurs when a user is sent an email with the intended purpose of coercing the user to reveal PI, open an attachment, or click on a link that leads to malware being loaded onto the user's system (NIST, 2013e); (b) password hacking, the act of a hacker discovering a user's password by guessing or using a tool to automate the attack on the password (Chapman et al., 2011); and (c) packet sniffing, which involves collecting information that flows over a network, which could include sensitive information or passwords (Chapman et al., 2011).

Once a hacker gains access to a system, using a particular user's information, he or she can utilize the privileges of the user. If the user has root access or administrative privileges, the hacker can gain greater control of the system (Chapman et al., 2011). With the elevated privileges, for example, administration rights or root level authority to a workstation or a server, a hacker can create a backdoor that allows him or her to gain access to the system, even if the hacker loses control of the user's machine. A hacker can

install a rootkit on a compromised system, giving the hacker control of the system (Chapman et al., 2011). When spyware or key loggers are installed on a user's system, the hacker can record the actions of the user and receive information that the user is generating (Chapman et al., 2011).

A Trojan horse is another form of malicious code that is disguised in information of potential interest to a user (Chapman et al., 2011). For example, a user could download an application that provides driving directions, but, in addition to the driving directions, the code is placing malware onto the user's system (Chapman et al., 2011). When the corrupt function is installed and executed, the malware works to infect other systems. Worms are similar to viruses but do not need user involvement to spread (Chapman et al., 2011).

Mobile devices also contribute to IT being susceptible to data loss (Leavitt, 2013). According to Leavitt, there are several potential threats to mobile devices, including unprotected data when a device is lost and data leakage to a public cloud or other destination. There has been explosive growth in smartphone sales, with smartphone shipments tripling in the last three years (Zhou & Jiang, 2012). However, the expansion of operating systems and device types creates new security threats and increases complexity for IT security professionals when applying security controls (Johnson & Pfleeger, 2011; Miller, 2011).

For instance, mobile device malware is generating a growing level of possible compromise as mobile devices host additional software and store increasing amounts of data (Felt, Finifter, Chin, Hanna, & Wagner, 2011). Based on the evaluation of four different products that detect malware, Zhou and Jiang (2012) found that, on more than

1,200 mobile devices over 14 months between 2010 and 2011, the malware detection software products detected a maximum of 79.6% of mobile malware that existed; in the worst case, they detected only 20.2%. In addition, malware attacks can have different “personalities.” Some malware is slow and quiet, with the goal of being undetected. Malware also may be fast and aggressive, intending to disrupt business (Dittrich, Bailey, & Dietrich, 2011). To add security protections to mobile devices, Leavitt (2013) suggested the installation of MDM, which provides an ability to set security policies for mobile devices and manage and monitor the security of a mobile device, and MAM, which secures a mobile application and controls application access to corporate networks and data.

The threat landscape changes as hackers advance their tactics, such as using botnets and DDoS servers to execute their attacks. Ablon, Libicki, and Golay (2014), in a report that focused on the marketplace for cybercrime tools and stolen data, were able to put prices on what hackers would pay for cybercrime tools. For instance, a hacker can buy a malware exploit kit for a couple thousand dollars (Ablon et al., 2014). Cyber hacking tools lower the level of knowledge the attacker needs to launch a cyber attack. In addition, the hacking community has moved to digital cryptocurrencies that offer anonymity. Examples of crypto currencies are Liberty Reserve, WebMoney, and Bitcoins (Ablon et al., 2014).

The propagation of malware is part of the changing threat landscape, and malicious code is at the root of much criminal activity on the Internet (Bayer, Kirda, & Kruegel, 2010). Bayer et al. estimated that, in 2010, there were 35,000 new malicious pieces of code daily. In 2013, the average number of malware rose to 82,000 per day (Bradley,

2014). Bayer et al. studied automated dynamic malware analysis systems, which will run suspect malicious code in a separate environment and assess whether the code is malicious by monitoring the actions of the code.

Browser isolation technology is a technology that prevents browser-based malware from infecting an institution's network. vSentry and LAVA are two products by Bromium (2015) that provide protection against malware. Bromium uses Intel's central processing unit (CPU) feature to create a virtual environment in a hardware isolated container, which provides malware protection to the user when inadvertently visiting a malicious Internet site or opening an untrusted document. vSentry automatically discards malware after the user completes his or her task, and LAVA provides attack visualization, giving the security analyst insight into what the malware was attempting to accomplish (Bromium, 2015).

Kancherla and Mukkamala (2013) created image visualization techniques to identify malware and obtained 95% accuracy on a dataset that contained 25,000 malware and 12,000 benign samples. The identification of malware provides companies an opportunity to eliminate the malware from information systems.

Technology companies also provided insights about malware attacks from breaches that they have investigated. Check Point (2013) analyzed security threats and provided a public report, available on the Internet, about their analysis. Specifically, the analysis was conducted on 356 companies worldwide, 40% of which were from the Americas; the finance industry represented 14% of the study participants. Check Point gathered the information over three months in 2012, utilizing network cloud monitoring data from a service that they provide. The Check Point report noted the change in hacker landscape

from lone individuals to well-funded structured organizations. In 63% of the organizations that Check Point studied, the organizations were infected with bots.

As previously noted, criminals use bots to infect large numbers of computers. These computers form a network, or a botnet. Criminals use botnets to send out spam email messages, spread viruses, attack computers and servers, and commit other kinds of fraud (Microsoft, 2014a; Yu, Gu, Barnawi, Guo, & Stojmenovic, 2015). Botnets are sold online for under \$100 each (Check Point, 2013), and they can spread viruses, distribute malicious software, steal data, attack computers, and send out spam, without the user's knowledge. Check Point's research showed that 63% of the organizations they studied were infected with botnets. However, if an organization does not know that they are infected with malware, they cannot mobilize their information security team to address the infection.

Check Point (2013) reported that, in 2012, there were 5,672 product vulnerabilities identified by vendors. The top three vendors with product vulnerabilities were Oracle, Apple, and Microsoft. The challenge of financial services companies is to patch all of these products in a timely manner to remediate the vulnerability for their company and not disrupt financial applications. Check Point's research showed that 75% of the companies in their study were not using the latest version of their software.

Check Point (2013) further noted that the ability to share data easily has added to the risk of data loss and reported that 80% of organization use free file-sharing software, such as Dropbox, Windows Live Office, YouSendIt, Sugarsync, and PutLocker, which allow users to share data outside the corporate network, which further increases the chance of data loss. Romer (2014) suggested that companies block free file-sharing

Internet sites to ensure the confidentiality and integrity of company data. In addition, companies are moving to greater utilization of social media sites, such as Facebook, Twitter, and LinkedIn (Check Point, 2013). However, hackers also are using these sites to deliver malware to users (Check Point, 2013). In Check Point's report, 61% of the financial industry companies had at least one potential data loss incident.

Check Point (2013) identified multiple areas in which technology can assist companies in protecting their data and systems. DLP is a technology that allows an organization to monitor outgoing data and to block data that meet defined criteria (Tahboub & Saleh, 2014). Cisco and McAfee both sell DLP solutions (Cisco, 2014c; McAfee, 2014b) that are capable of blocking data elements like social security numbers, bank account numbers, and healthcare data from being sent in clear text within emails (Check Point, 2014c). DLP solutions search for patterns in data, or a specific tag added to a document, and can either monitor and log that the data left the company through email or the Internet, or block the data transmission. Security analysis can monitor the data blocked or transmitted that fit the policy that was defined within the DLP product (CA Technologies, 2015; Cisco, 2014c; McAfee, 2014b).

Firewalls have added more granularity and insight into the data that are being transmitted (Snyder, 2012). One example is the Palo Alto (2015) next-generation firewall, which provides the ability to understand and block specific applications and users from transmitting data. Next-generation firewalls can identify what applications are allowed to utilize specific resources, thereby reducing the chance of malicious rogue malware exfiltrating data from a company (Snyder, 2012). Next-generation firewalls could be used by financial services network security teams to stop the flow of specific

data from an application or user when the security team suspects that the system or user has been compromised (Snyder, 2012).

However, Snyder (2012) explained that the additional power of the next-generation firewalls adds complexity over traditional firewalls, and this complexity could create miscoded rules, leading to security incidents and making the environment more difficult to manage. Increased granular controls at the firewall layer could help prevent data security incidents and breaches (Snyder, 2012). Companies can outsource their next-generation firewalls to a service provider. One example is Dell SecureWorks, which will run and monitor the security of firewalls (Dell, 2014). New technology innovations provide companies additional capabilities for protecting data.

IBM provides an annual report on security and risk (IBM, 2013). IBM X-Force is a research and development team focused on computer security threats, vulnerabilities, and data protection (IBM, 2013). To conduct the analysis of security threats, IBM utilized IBM Managed Security Services data to identify security threats associated with botnets, application vulnerabilities, and spam. IBM Managed Security Services provide a set of security services that companies can outsource. IBM's set of services includes mobile endpoint protection services, firewall management, identity and access management, and DDoS monitoring and protection (IBM, 2014b). To address security threats, IBM suggested several investments in technology that they sell, such as identity and access management tools, managed security services, and security information and event management products, to protect data and ensure that only authorized personnel can access data (IBM, 2013).

McAfee (2012, 2015) publishes a quarterly report on security threats, which showed an increase in incidents of mobile malware and mobile spyware. In the last quarter of 2014, McAfee (2015b) identified over 6 million different mobile malware signatures. Ransomware is one such instance of malware; it takes control of a system, after which hackers require payment to unlock it (Microsoft, 2014b). In the second quarter of 2015 McAfee (2015b) identified 1.2 million new ransomware samples, for a total of over 4 million. This represents a 25% growth in ransomware samples in 2Q 2015 (McAfee, 2015b).

Cryptolocker is a specific instance of ransomware, where the attacker encrypts files on a user's device and demands payment for the files to be decrypted (Mustaca, 2014). Jeffers (2013) reported that, between September 2013, when Cryptolocker was first identified, through December 2013, Cryptolocker grossed \$30 million in ransom payments. To assist users who become compromised by Cryptolocker, some technology vendors have offered free services to unencrypt systems that have been infected with Cryptolocker malware (Seltzer, 2014).

As more businesses and users move to mobile devices, so will the hackers, as noted by the growth in Android malware (McAfee, 2012; Mearian, 2013). Mearian reported that mobile malware, mainly targeting the Android operating system, increased by 614% from March 2012 to March 2013. Androids represented 52% of the mobile device market in 2012 (Mearian, 2013). Zheng, Sun, and Lui (2013) applied security analytics to mobile devices. They implemented DroidAnalytics, a signature-based analytics system to collect, manage, analyze, and extract Android malware. In analyzing 150,368 Android applications, their solution was able to identify 102 different families of Android

malware, with 327 specific zero-day malware instances. Further, Peng, Wang, and Yu (2013) developed a model to study the propagation of malware on mobile devices spread through social networks. Their work provided understanding on how worms would spread on mobile devices based on the social networks in which a user participated. As smartphones grow in usage and functionality, they are enticing targets for hackers and malware writers (Peng et al., 2013).

Technology exists to help companies defend against attacks. FireEye (2013b) is a security company that provides technology that allows the user to execute suspect email attachments and links within emails in a virtual environment to determine whether they are malicious. According to the Senate analysis of the Target breach (U.S. Senate, 2014), the FireEye solution, which provides dynamic malware protections, recognized the attack, but the Target staff did not follow through to address the threat information. In another instance, the FireEye (2013a) threat report indicated that FireEye appliances located in a financial services sector detected malware events that penetrated the perimeter security 10 times per hour, demonstrating that the financial services sector is under constant malware attack. FireEye (2013a) determined that, in 92% of the cases, malware is delivered as an email zip file attachment.

Cyberwar and cyber attacks are concerns to industry and governments (Elliott, 2011; Fidler, 2011; Parks & Duggan, 2011). With several cyber attacks being reported in the media, such as Stuxnet and DDoS attacks against Estonia and Georgia, cyberwar is no longer a hypothetical attack scenario (Elliott, 2011; Fidler, 2011; Parks & Duggan, 2011). One issue that makes cyberwar more complicated than a traditional war is the difficulty

in identifying the attacker (Elliott, 2011; Fidler, 2011; Parks & Duggan, 2011). Nation state cyber threats are a risk to Fortune 500 financial services companies.

In the spring of 2013, the media reported DDoS attacks against the U.S. banking community, including such financial institutions as American Express, Ameriprise Financial, Bank of America, BB&T, Citizens Financial, PNC, and KeyCorp. The DDoS attacks achieved sustained floods of 70 Gbps and 30 million packets per second (Schwartz, 2013). Defending against these security data breaches and external threats is an ongoing challenge (Kitten, 2013), and the FFIEC has directed banks to combat DDoS attacks by monitoring Internet traffic, having a DDoS response plan, ensuring proper staffing to execute the DDoS response, and sharing information about the attack with FS-ISAC (Messmer, 2014).

In 2014, Sony Pictures Entertainment fell to a targeted malware attack, instigated, according to the FBI, by North Korea. The malware used to attack Sony erased all computer hard drives. The attacker took copies of internal documents and movies and released the information to the public (Krebs, 2014). Researchers who work at Computer Emergency Readiness Team (CERT) at Carnegie Mellon University developed an assessment tool that allows a security incident responder to assess the risk of an attack and identify a response plan (Connell & Waits, 2013). The assessment tool is loaded with the roles and responsibilities of the team and the critical data on the system. The goal of the tool is to identify the threat and quickly respond before the malicious code has time to propagate in the system.

Business Enablement IT

Technology continually advances, giving more options to support changing business models. Two examples of technology advances are cloud computing and mobile device usage and capabilities (PwC, 2013). Cloud providers are focused on security because a security breach could ruin their business, and, indeed, there have been only a few cloud security breaches to date (Banham, 2014). Microsoft Business Productivity Online Suite had a breach in 2010, where customer data could be accessed by someone other than the owner, and, in 2013, GoGrid disclosed that an unauthorized third party may have viewed account information (Banham, 2014).

In yet another example of security breaches, fraudsters are using stolen PI to create Apple Pay credentials to buy merchandise at participating merchants (Krebs, 2015). Further, mobile banking applications are a vector of security vulnerabilities. Constantin (2014) reported that, in the analysis by IOActive of the mobile applications of 60 financial institutions, none of the applications detected that the device was jailbroken, i.e., had allowed the operating system to bypass security controls (Constantin, 2014). Further, 40% of the financial mobile applications analyzed did not validate the authenticity of the digital certificate, making the application vulnerable to man-in-the-middle attacks (Constantin, 2014). IOActive suggested several actions to improve the security of financial mobile applications, including the use of secure transfer protocols, encrypting sensitive data, and detecting jailbroken devices (Constantin, 2014). As companies exploit new technology, new security threats emerge, and new security technology solutions are created.

Amoroso (2013), the chief security officer at AT&T, explained how the technology evolution set the stage for business process changes, which resulted in an increase of information security challenges. Amoroso explained, as companies started to utilize email as a mechanism to communicate to external parties, external email forced companies to open network ports and accept traffic from outside the company's network. External email created the security challenges of additional attacks within the company's network, including spam, malware embedded in email, and the risk that an employee could send sensitive data through external email, creating data loss and possibly creating a privacy breach if the data were in the scope of privacy regulations.

Amoroso (2013) explained that, to defend against the new security threats, companies need to add such technology as anti-spam, anti-virus, anti-malware, DLP, and intrusion prevention systems (IPSs) to their computers. Further, according to Amoroso, there has been a growing number of mobile devices and the functions that they can perform. The increase in the use of mobile devices creates a threat to perimeter security by creating additional network connections on a corporate network, as well as vectors for outgoing data. Many of the mobile devices have integrated public cloud services to back up information, which creates additional data protection challenges for a company. To provide control over corporate assets on mobile devices, technologies such as MDM and MAM are being utilized (Leavitt, 2013).

Amoroso (2013) suggested implementing tiered network architecture to address the expanded information security challenges that companies face. The core network would contain firewalls, IPSs, DLPs, anti-virus, anti-spam, anti-malware, SIEM, and access management (Amoroso, 2013). A tiered network design would allow critical business

data and programs to be separated from less critical systems and data. Amoroso advised that highly robust security technology and architecture will enable businesses to take advantage of cloud and mobile technologies. An example of failed network segmentation is the Target data breach (Vijayan, 2014b). The Target network design allowed the breach to start from a third-party HVAC system, which ultimately gained access to point-of-sales devices (Vijayan, 2014b).

Cloud environments have five unique characteristics, including on-demand self-services, access through the Internet, resource sharing, elasticity, and monitoring (Idrissi, Kartit, & Marraki, 2013), to be considered to reduce the chance of data loss (Ballabio, 2013). Businesses are moving workloads to cloud environments for many positive security reasons: (a) cloud environments are large and highly distributed, which provides added protection to deflect cyber attacks; (b) cloud infrastructures are highly redundant, providing added resiliency in a cyber attack; and (c) load balancing creates sophisticated fail over capabilities that could be utilized under a security attack (Ballabio, 2013).

Grobauer et al. (2011) provided an overview of the information on security threats for cloud environments. As companies consider utilizing cloud technology, they need to consider the risks and the benefits of doing so. Some examples of security risks related to cloud technology are data protection, data disposal, physical controls, access controls, logical controls, and reporting obligations (Cadregari & Cutaia, 2011). Grobauer et al. defined cloud vulnerabilities to include attacks on the virtual machine, session hijacking, and Internet protocol vulnerabilities. NIST created guidance when using cloud environments (NIST 800-146, 2012). NIST highlights several open issues that consumers should consider when utilizing public cloud services. Issues that should be considered are

that the consumer retains the responsibility for regulatory compliance, the lack of visibility within the cloud service, and the challenge of forensic support.

Alfath, Baina, and Baina (2013) identified unique security risks for cloud environments, including (a) multiple tenants' data coexist, (b) enterprises lose control of their data, (c) there is a lack of security guarantees, and (d) public infrastructures make clouds more vulnerable to attack. Eken (2013) highlighted several cloud security threats, such as increased complexity, the lack of ability to conduct investigations on who accessed data, data comingling between different companies, reliance on the cloud provider for data backups, unsecured data transfer between the company and the cloud provider, and unsecured data disposal.

A cloud provider's environment is complex due to the need to separate and secure multiple users' data (Khalil, Kreishah, Bouktif, & Ahmed, 2013). One of the technical underpinnings of the cloud environment is virtualization of physical resources that logically separate workloads and environments (Jin et al., 2015). Duncan, Creese, Goldsmith, and Quinton (2013) provided insights into hypervisor attacks. A hypervisor is a piece of software, firmware, or hardware that creates and runs one or more virtual machines on a host machine (Lee, 2015). Attacks include disabling the hypervisor, gaining control of a virtual machine, or attacking a sibling virtual machine. A virtual machine is a software image that is contained on a host computer, managed by a hypervisor, providing isolation from other virtual machines on the same hardware (Lee, 2015).

A cloud provider likely would have more privileged users with access to the infrastructure. The cloud environment could lead to more risk from network attacks,

account hijacking, privileged user access, and data disposal (Grobauer et al., 2011; Khalil et al., 2013). To access the cloud, the user needs to communicate through the Internet, which is untrusted (Grobauer et al., 2011; Khalil et al., 2013). There is a possibility that the network flow to a cloud could be open to vulnerabilities, such as a man-in-the-middle attack, where the hacker is positioned between the users and the destination, intercepting communications (Grobauer et al., 2011; Khalil et al., 2013). Cloud providers host several companies on their infrastructure, so there are risks of data being exposed if the cloud service does not securely erase data before reallocating space to another company's workload. Encryption is one method that cloud providers and companies that participate in public cloud services can utilize to protect data from unauthorized use (Grobauer et al., 2011; Khalil et al., 2013).

Insider attacks from within the cloud service provider, such as sharing employee security background check information with other customers, also are a risk (Duncan, Creese, & Goldsmith, 2012). Additionally, the customer of a cloud service may be unaware of the cloud provider's policy on bring your own device (BYOD). An unmanaged BYOD device could be compromised with malware, and the cloud service provider would be unaware of the threat. If an endpoint, for example a key logger, is compromised, customer data could be compromised (Duncan et al., 2012). Further, unless the cloud customer encrypts its data, the cloud providers may have the ability to read it (Duncan et al., 2012). When considering a cloud service, confidentiality of data is an important consideration (Jenkins, 2013). Analyzing encryption alternatives includes deciding what data need to be encrypted and securing the management of the encryption keys (Jenkins, 2013). Products that provide the customer of a cloud service the ability to

manage and control encryption keys include CipherCloud (2014), which allows a cloud user to encrypt data in the cloud but render the data decrypted when displayed within the enterprise.

Cloud security may provide challenges in addition to solutions. Frost & Sullivan, in partnership with Booz, Allen, & Hamilton, conducted a study of over 12,000 information security professionals; of the respondents, 56% believe that their security organizations were understaffed (Suby, 2013). However, cloud providers, like Amazon Web Services (2014), provide many built-in security services that companies can utilize, which decreases the security burden of their staff. Examples of Amazon Web Services' security capabilities include built-in firewalls, multi-factor authentication, private network subsets, encrypted data storage, and hardware-based crypto-key storage.

Computer services that help companies assess and monitor cloud services also are available. McAfee (2014c) offers cloud security verification services, from deep dive testing of the cloud infrastructure to daily security scans of the cloud environment. To help customers feel more comfortable with cloud computing, researchers proposed a trust-aware framework to evaluate the security of a cloud environment (Habib, Varadharajan, & Muhlhauser, 2013). The trust-aware framework utilizes the trusted platform module in hardware, combined with the consensus assessment initiative questionnaire developed by the Cloud Security Alliance (CSA), to provide assurance of the cloud provider's security (Habib et al., 2013).

Mobile devices are rapidly being incorporated into enterprise solutions (Li & Clark, 2013). Companies need to protect their employees' mobile devices, as they present security challenges that are similar to those of desktop computing environments (Li &

Clark, 2013); e.g., mobile devices can be infected by malware through an Internet link a user clicks on or through an infected application the user downloads. Companies must create a secure environment to support business requirements on these mobile platforms (PwC, 2013). Mobile variants of anti-virus software are available on some platforms, but mobile operating systems may not allow for independent security solutions on a specific vendor's operating system.

The proliferation of mobile applications creates additional security exposures; e.g., it is easy for users to download new applications to their inadequately secured mobile device. Mobile operating systems, for example, Apple's iOS, have the ability to be jailbroken, bypassing device security (Li & Clark, 2013). Romer (2014) highlighted that the focus should be on protecting the business data. Multiple vendors provide a capability to separate corporate and personal information on a mobile device (containerization), which provides additional data protection of company assets (Airwatch, 2014; Good, 2014, Hernandez, 2014). With containerization capabilities, companies can control data by storing company information in an isolated container on the mobile device. By utilizing MDM and the containerization capability, companies have the ability to monitor the security of the device, control what applications can be loaded onto the mobile device, remotely wipe the content if the device is lost or stolen, and provide isolation and controls for corporate data (Romer, 2014).

Willems (2013) described why the Android platform is a sought-after target for hackers. As of 2013, Android had approximately 75% of the smartphone market; therefore, any malware targeted toward Android devices would have a large install base. Android applications are not vetted by any organization, and users have the ability to

install applications to their device. These two characteristics make Androids susceptible to hackers (Willems, 2013), and, therefore, researchers are looking for ways to detect malicious code on smartphones. Further, Dixon and Mishra (2013) analyzed how the rate of battery drain could be used to detect malicious code on a smartphone.

BYOD brings added security threats (O'Neill, 2014). In addition to users losing mobile devices more frequently than PCs, thieves understand that, as well as personal data, there is often corporate data stored on the device, or access to corporate systems is allowed through the device (O'Neill, 2014). Steiner (2014) proposed a multi-pronged approach to secure mobile BYOD devices, including the use of authentication tokens for the web, application, and data access; tight integration with the corporate access rights directory; and storing corporate content on the corporate network.

Security Analytics IT

Companies are realizing they could have a security breach and not be aware it occurred (Verizon, 2013). Verizon reported, in 54% of the data breaches they investigated, it took months from the point of initial compromise to the discovery of the data breach. Ponemon Institute (2015) published a study providing data about how fast breaches were detected. The mean time to identify a breach was 206 days. The mean time to contain a breach was 69 days. Financial services companies are investigating methods to detect data breaches closer to the time of compromise. The earlier a security compromise can be detected and remediated, the smaller the window of time exists for exfiltration of data or use of the information by the attackers for their specific purposes (Radcliff, 2012).

Hackers may breach systems for the purposes of sending spam, attacking other systems, or stealing data. One technology being used to detect system compromises and prevent security incidents is SIEM tools, which provide the capability to aggregate data-finding patterns or suspicious activities (Chickowski, 2011; Lozito, 2011; Oltsik, 2013). The SIEM market is growing: In 2012, the SIEM software market grew 27.5%, and the SIEM appliance market grew 11.9% (Messmer, 2013).

Tankard (2014) described the changing landscape of hackers and the need for security analytics. Tankard explained that hackers today are using the same cloud services that businesses use to lower the suspicion of the location of the attack—which could be a well-respected cloud services provider. Tankard suggested that understanding what data are important and using security analytics to understand the use and flow of high-value data are approaches that could be used to increase the company's ability to detect a breach.

Security analytics are evolving to utilize new technology. Cardenas, Manadhata, and Rajan (2013) suggested that the current SIEM tools are too restrictive because they rely on structured data that require defined schemas. They believe that tools that can deal with large-scale unstructured data, like Hadoop, are the next-generation security analytic tools.

Enhanced Security Control IT

Researchers continue to find new ways to address security issues. When new information technology solutions are enabled for example cloud, mobile, or new business applications, financial services sector companies need to assess if additional security

solutions are needed to support new IT capabilities. The following are examples of how emerging technology and research can provide additional options for financial services sector companies to decrease their data security risks.

Koch, Holzapfel, and Rodosek (2011) developed an approach to keep private the data that are stored on social media sites. The researchers created an architecture that provided an encryption extension to the Mozilla Firefox web browser that transparently encrypts all data stored on their social media servers. The authors explained that their goal was to produce an easy-to-use solution that could keep data private when stored in a web browser. This type of approach protects data stored outside the enterprise and would reduce the chance of data breaches. Multiple vendors offer this capability (Bromium, 2015; Spikes, 2015).

Phishing attacks can compromise user devices through an email that attempts to mislead the user by disguising the real source of the email and tries to coerce the user to open an attachment or click on a link (Herzberg & Margulies, 2012). Researchers are exploring alternate ways to authenticate users and devices to reduce the possibility of being deceived and prevent the use of stolen authentication information (Herzberg & Margulies, 2012). Products available today, such as McAfee's (2013b) email protection, can help companies to reduce phishing attacks. In addition, Sender Policy Framework (SPF) reduces abusive emails and detects forgery by allowing recipients to verify the sender's identity, and Domain Keys Identified Mail (DKIM) allows a sender to cryptographically sign the contents of an email and confirm where the email originated. Domain-based Message Authentication, Reporting, and Conformance (DMARC)

leverages SPF and DKIM by allowing a company to publish an email policy that declares the rules the company uses to determine valid email.

According to Imperva (2012), current anti-malware solutions detect fewer than 5% of newly created viruses. To address the malware detection gap, new approaches are needed. Xu, Yao, Ma, and Crowell (2011) published an approach to detect malware by incorporating system and end-user behavior analysis. The researchers were addressing the charge that 10% of the websites they analyzed contained drive-by-download malware, i.e., malware deposited on a user's machine when the user visits an infected website. Xu et al. focused on file and process creation, monitored file system events and user actions, and found patterns in the relationship of the users' actions and system events. Using this approach, the researchers could detect malware earlier in the cycle, at the onset of the infection. The approach does not rely on new anti-virus signatures, and it provides improved malware detection. End user behavior analytics is seeing growth. In a paper by Gartner (2015) assessing the market landscape of user and entity behavior analytics, they identified multiple solutions seeing high growth. Solutions analyze current behavior and detect changes in behavior. Some of the products that Gartner identified providing solutions in end user behavior analytics were Dtex, SpectorSoft, Bay Dynamics, ObserveIt, and SureView.

As financial companies utilize cloud computing, security risks should be considered (Ginovsky, 2013; Jenkins, 2013; Kothari, 2013). Ibrahim, Hamlyn-Harris, Grundy, and Almorsy (2011) explained that, in a cloud IaaS environment, the cloud provider does not have control over or insights into the contents of the hosted Virtual Machine (VM). VMs could be compromised, and the compromised VM could attack the other VMs or the

hypervisor. Consequently, Ibrahim et al. proposed a model that would provide transparent and real-time security monitoring of VMs in the cloud.

Security Information-sharing Forums

With the growing complexity of cyber attacks, security personnel are sharing information regarding attacks with their peers. Industry-specific ISACs allow members to share information with some level of trust (Moriarty, 2011). ISACs include member groups focused on the following sectors: communications, energy, emergency management, financial services, healthcare, transportation, IT, maritime, nuclear, public transit, research and education, supply chain, and water (National Council of ISACs, 2013). Security information-sharing forums could make financial services companies aware of a data breach or incident they were previously unaware of.

FS-ISAC (2013a) was created in 1999 in response to Presidential Directive 63, which mandated public and private sector information sharing of physical and cybersecurity threats and vulnerabilities to help protect U.S. critical infrastructure. Through FS-ISAC's Critical Infrastructure Notification System (CINS), alerts can be sent to members in near real time. FS-ISAC provides a method to share anonymous information across financial services members, allowing the company to not disclose their identity. The U.S. Department of the Treasury, the Office of Comptroller of Currency, the Department of Homeland Security, and the U.S. Secret Service recommend that financial services companies join FS-ISAC, which requires a paid membership to belong.

The mission of FS-ISAC (2013a) is to work collaboratively with the government and financial services sector to share cyber threat information, with the goal of improving the security within the financial services sector. Working together the Department of the

Treasury, the Financial Services Sector Coordinating Committee and FS-ISAC enhance the ability of financial services to prepare for and respond to a physical or cyber threat. An example of the work that FS-ISAC does was highlighted in an interview with Bill Nelson, the president of FS-ISAC (Kitten, 2013). In the interview, Nelson explained how FS-ISAC is working across the financial services sector to combat account takeovers and DDoS attacks by using technology for anomaly detection. FS-ISAC has partnered with Depository Trust & Clearing Corporation (DTCC) to create a new company with a mission to provide automation and services to aid the automatic ingestion of threat information (Soltra, 2015).

InfraGard (2015) is a partnership between the FBI and the public and private sector. InfraGuard has identified the financial services sector as one of the 16 critical infrastructures. State and local law enforcement, academia, and businesses are involved in the InfraGard mission to prevent hostile acts against the United States. Of the Fortune 500 companies, 300 have representatives involved with InfraGard.

The Internet Crime Complaint Center (IC3; Federal Bureau of Investigation, 2014) is a partnership between the FBI and the National White Collar Crime Center. Its mission is to receive, develop, and refer criminal complaints in the area of cyber security. The IC3 also partners with law enforcement and regulatory agencies.

Sharing forums may not provide all of the benefits needed. Ring (2014) explained that attacks are becoming increasingly personalized, which would make information sharing of limited value. Ring also stated that threat intelligence sources have a high rate of false positives, requiring additional work for financial services to investigate, also providing limited value. However, overall, sharing forums may provide information to

financial services companies to prevent cyber attacks, or the information may provide intelligence to allow the company to discover that a successful attack has taken place.

Best Practices

NIST (2013a) was founded in 1901 to promote U.S. innovation and industrial competitiveness. The organization consists of approximately 3,000 employees and 2,700 visiting professionals from academia and industry. It has a wide range of scope, but its four top focus areas are cybersecurity, power grids, electronic health grids, and cloud computing (NIST, 2013a). NIST plays a key role in protecting the critical infrastructure from cyber attacks and produced a standard for cybersecurity that was published in February 2014 in support of the 2013 Presidential Executive Order. Some financial services companies have been identified as critical infrastructures and are required to comply with the NIST cybersecurity standard (Roman, 2013).

One method that NIST (2013b) uses to advance security best practices is to produce standards and guidance for the public and private sectors. In the area of information security, there are many NIST standards, including malware prevention, security patching, protection of PII, intrusion detection and prevention, cloud computing, and mobile security, to name a few (NIST, 2013b). In addition to standards, NIST utilizes other methods to advance their areas of interest and influence private industry. For instance, in April 2013, NIST announced the creation of the National Cybersecurity Center of Excellence (NCCoE). The NCCoE is a public-private partnership to help industry secure data and digital infrastructure. Eleven private industry companies have joined NCCoE to help combat the cybersecurity challenges (NIST, 2013f).

NIST offers many publications that provide best practices and guidance to government agencies and industry. NIST Publication 800-83 (NIST, 2013c) is a guide to malware incident prevention and handling for desktops and laptops. Having an approach to address malware is very important to prevent data breaches, as 37% of breaches are attributed to malware (Mello, 2013). NIST Publication 800-83 defines malware as malicious code that covertly inserts a program into the system with the intent to steal or destroy data or run intrusive programs, which can cause widespread damage or disruption.

Examples of malware described by NIST (2013c) include (a) a virus that inserts copies of itself into a host program or data files; (b) worms, self-contained programs that propagate without involvement from the user; (c) Trojan horses, which appear to be something that they are not, leading the user to be unaware of the malicious code; and (d) malicious mobile code, software transmitted to the mobile user, typically without the user's instruction.

An example of a virus is the Gozi virus, discovered in 2007 (Smith, 2013). Hackers utilized a PDF file to transport it and when the user opened the file, the virus was installed. The virus was focused on stealing bank account numbers, usernames, and passwords. It is estimated that the Gozi virus accessed accounts resulting in the theft of tens of millions of dollars (Smith, 2013).

Conficker, which was discovered in 2008, is an example of a worm. Conficker originally infected Windows system files to target users of networking sites, such as Facebook, and mail sites, such as Yahoo, and moved to file shares and removable media. It is estimated that Conficker infected seven million computers (Kirk, 2012).

Neverquest is a Trojan piece of malware that is spread through malicious email or social media sites and is used to steal money from a user's bank accounts. It collects banking information and, can transfer money or change the user's credentials (Kassner, 2013).

NIST also described multiple attacker tools, including: (a) backdoors, which allow the attacker to have access to the system without the knowledge of the system owner; (b) keystroke loggers, which transfer data, such as passwords, that are typed into the system; (c) rootkits, which install code on the host in such a way that they are difficult to find; (d) web browser extensions that monitor all browser traffic; and (e) email generators that create spam sent from the victim's computer (NIST, 2013c). NIST provides technical approaches to detect and defend against malware.

Constantin (2013) described the possible negative effects of a malicious web browser extension, which can insert rogue code on a computer to place malicious advertisements in web pages or hijack a search query. The end user can be infected with malicious code that could lead to stolen credentials and hijacked accounts, or to bypass two-factor authentication (Constantin, 2013). In 2014, AOL was hacked, and email accounts were compromised (Albanesius, 2014). AOL user accounts had their address books harvested, and fake, malicious email was sent, appearing to the recipient that the mail came from the (compromised) user's account (Albanesius, 2014).

NIST (2013c) described the change in malware over the last several years, from fast spreading and easy to notice to stealthy and quiet, making malware more difficult to detect. Malware continually changes, and companies need to utilize IT and information security best practices to combat it (Dispensa, 2010). NIST suggested organizations

utilize such technology as anti-virus software, intrusion prevention systems, firewalls, content filtering and inspection, and application whitelisting to assist with threat mitigation.

NIST (2103c) recommended organizations consider more defensive technical approaches to decrease the likelihood of malware infections by using technology such as sandboxing, browser separation, and segregation of computer resources. Detection approaches are suggested to analyze systems by looking for patterns in anti-virus and intrusion prevention systems (NIST, 2013c). SIEM technologies provide consolidated log file and system alert correlation providing organizations a method to identify systems infected by malware (NIST, 2013c).

Patch management, identified by NIST (2013b) as the process of identifying, acquiring, installing, and verifying patches for products and systems with known security vulnerabilities, is a key security measure for organizations. Technology also can assist organizations with the patching process. Patching technology includes scanning tools that provide insight into what patches are needed for host systems and network monitoring, which can identify applications that need patches (NIST, 2013b). Further, patch management technology can bundle patches for distribution and install software (NIST, 2013a). Technology also can automate certain parts of the patching process to ensure that systems are kept to the desired levels (NIST, 2013b). However, patches also can cause applications to have failures. In November 2013, Microsoft released two patches to Outlook that created problems with the Outlook application, and Microsoft directed its customers to not install the patches until the company could remediate the issues (Leonhard, 2013).

Protecting PII is a goal for all organizations subject to regulations related to safeguarding individuals' privacy (NIST, 2010; U.S. Department of Health and Human Services, 2013a). NIST's Publication 800-122 provides guidance on how to protect PII (NIST, 2010). Financial institutions are within the scope of state privacy laws because they hold such information as individuals' bank account numbers, date of birth, social security number, and mother's maiden name. In most states, regulations require companies to report PII loss if the data was not been encrypted (National Conference of State Legislators, 2013).

Focusing on the technology opportunities, NIST (2010) suggested that de-identifying information reduces the risk of data loss or misuse. De-identification of data refers to eliminating the link to a specific person (Future of Privacy Forum, 2014). In addition, techniques to mask or replace data provide the ability to protect PII (NIST, 2010). Multiple companies provide data-masking technologies to hide sensitive data (Oracle, 2015; SafeNet, 2015; Vormetric, 2015). Tse (2014) defined data masking as the act of hiding the actual data so that an unauthorized user cannot decipher them.

Data masking technology is available in multiple forms. Static data masking, which is the most mature, provides masking of data prior to use. Static data masking is often used in test environments, where application tests are performed to verify the function of the application, and where the desire is to simulate a production environment without exposing sensitive data to the testers (Feiman & Casper, 2012). Dynamic data masking provides obfuscation of data in real time, and data redaction masks unstructured data, such as PDF, Word, and Excel files (Feiman & Casper, 2012).

NIST Publication 800-94 (NIST, 2012b) also provides guidance for intrusion detection and prevention systems. An intrusion detection system (IDS) is software that automates the detection of an attack or malicious piece of code. An IPS has similar capabilities to IDS systems, but can also stop possible security incidents. An example of an IPS stopping an attack was published by Cisco (2014d). Using Cisco's own technology, they were able to detect a new variant of the Rinbot virus and develop an IPS signature to stop the virus (Cisco, 2014d). Cisco then distributed the signature to their customers so that they also could combat the Rinbot virus (Cisco, 2014d).

An IPS has the ability to terminate network connections that are being used in an attack, block access by the attacker's IP address, and block access to internal or external hosts and applications. NIST (2012b) describes multiple types of IDS and IPS capabilities, including: (a) network-based monitoring devices, usually deployed at network boundaries, which can monitor network traffic for suspicious activities; for example, network-based IPS can set up rules to block source IP addresses, or network ports; (b) wireless monitors, which can analyze wireless network; (c) network analysis, which examines network traffic for unusual activities; and (d) host-monitoring analysis, which monitors hosts for suspicious activities.

NIST (2012b) described several functions that IDSs and IPSs can provide to detect and prevent malicious network traffic. Threshold values allow the support team to set a range of normal values and be alerted when an event hits a specified limit; for example, 20 failed attempts to connect in 60 seconds would generate an alert. Blacklists can be used to block traffic from certain destinations, and whitelists can be used to identify trusted systems (NIST, 2012b).

Gartner (2014) predicted a 5% growth in mobile phone shipments, estimating that 1.9 billion mobile phones would be shipped in 2014. NIST (2013d) provided security guidelines for mobile devices, including: (a) deciding what level of security needs to be active for a mobile device to be connected to a company network; (b) deciding what corporate applications will be allowed on a company-owned and personally-owned mobile device, (c) encrypting data on a mobile device, (d) having the ability to wipe corporate data on a mobile device, and (e) detecting when security settings are altered.

In February 2013, President Obama issued an executive order that focused on improving the U.S. critical infrastructure in the face of growing cyber attacks (White House, 2013). The president called for NIST to develop a framework to reduce cyber risk, and, in response, NIST published the Framework for Improving Critical Infrastructure Cybersecurity in February 2014 (NIST, 2014b). The government is coordinating the adoption of the new NIST cyber standard, whereby companies could be required to adopt it due to their being identified as part of the critical infrastructure.

Trope and Humes (2013) provided a legal analysis of the cybersecurity executive order. According to Trope and Humes, the executive order is aimed at improving a company's ability to withstand a cyber attack and/or limiting the damage caused by it. Trope and Humes explained that the cybersecurity executive order currently calls for voluntary compliance. Nonetheless, the order could put pressure on companies that are identified to be part of the critical infrastructure to improve their cybersecurity. Major electricity generation and distribution facilities, financial services, and transportation providers are examples of critical infrastructures (Trope & Humes, 2013).

According to Trope and Humes (2013), the U.S. government can notify companies of an identified threat in two ways. An Imminent Target Notice provides a method for the U.S. government to communicate to a company that there is a specific cyber threat that is targeting it. Catastrophic Target Notices provide the ability for the U.S. government to inform companies that a cybersecurity incident could reasonably occur that affects the nation. Trope and Humes stated, with the new cybersecurity executive order, companies would be under pressure by their board of directors to ensure that investments in cybersecurity are not delayed. However, until there is case law related to the cybersecurity executive order, companies will not know the government's level of expectations or the government's ability to enforce an Imminent Target Notice or a Catastrophic Target Notice (Trope & Humes, 2013). In addition, it is unclear the level of responsibility to which a company will be held accountable if they are defined as part of the critical infrastructure (Trope & Humes, 2013).

In May 2013, New York Governor Andrew Cuomo initiated an inquiry to the largest insurance companies that serve the state's citizens with regard to their cybersecurity program (New York State, 2013). Specifically, 31 insurance companies were asked to disclose any instances of cyber attacks, their current technical capabilities to detect and defend against cyber attacks, the number of people and investments targeted to support cybersecurity, and the board of director's oversight to cybersecurity. In 2013, New York State held a cyber security competition among 200 banks to understand and provide relative preparedness for a cyber attack (Chaudhuri, 2013). New York State indicated that it hoped to utilize the same tool for insurance (Chaudhuri, 2013).

Multiple state and federal regulations require companies to disclose data breaches (Mintz Levin, 2015; National Conference of State Legislators, 2013; Singer, 2013). In the absence of overarching federal data breach notification laws, all states except Alabama, Kentucky, New Mexico, and South Dakota have passed legislation that requires businesses to disclose information about security breaches (National Conference of State Legislators, 2013; Singer, 2013). Public Internet sites, such as the Privacy Rights Clearinghouse (2015), and Data Loss db (2014), provide a history of data breaches. For specific types of data, for example, health data, the U.S. government requires HIPAA-regulated companies, such as doctors and hospitals, to disclose data privacy breaches (U.S. Department of HHS, 2013b).

The Gramm-Leach-Bliley Act (GLBA) of 1999 requires financial institutions to provide customers with copies of their privacy policies and to safeguard customer data (Stevens, 2012). Financial institutions are required to anticipate threats that could lead to client's harm (Stevens, 2012). The FTC has jurisdiction over the GLBA, and the FTC holds financial institutions accountable to assess reasonably foreseeable threats and require the institution to update policies, procedures, and controls to protect customer data (Stevens, 2012). Financial institutions also are required to monitor, evaluate, and adjust their information security program against regulations and industry best practices (Stevens, 2012).

The FTC has the general authority to levy penalties on companies that do not adequately protect consumer data (Stevens, 2012). The requirements include the need to design and implement a safeguard program and to evaluate and adjust the program as needed (FTC, 2006). The penalties can range from monetary fines to consent orders that

require companies to implement information security programs (Stevens, 2012). An example of an FTC violation of GLBA concerned Franklin Budget Car Sales Inc. and debt collector EPN Inc. The two companies were found to have peer-to-peer file sharing software installed on corporate systems, which led to exposing the PII of thousands of consumers; the settlement required both companies to implement comprehensive security programs (Nonaka, 2012).

Breaux and Baumer (2011), in a 10-year retrospective on rulings made by the FTC, suggested companies must implement a continuous security improvement program requiring ongoing assessments of emerging risks and utilization of industry security best practices. Several factors influence IT security investments, including regulations, business enablement, and the changing security threat landscape (Breaux & Baumer, 2011). Current federal regulations require a business to have reasonable security controls, but the expectation of what is reasonable may change over time (Breaux & Baumer, 2011).

One of the ways the U.S. government communicates its view of security best practices is through publications of regulations and guidelines. Some examples of federal regulations pertaining to security and data protection requirements can be found in the HIPAA, GLBA, and FTC Act (Stevens, 2012). The FDIC's (2014) Compliance Manual defines requirements to comply with GLBA. The manual states the institution will be audited to ensure a stable compliance audit program exists, that steps are taken to correct deficiencies, and audits happen with appropriate frequency.

International Organization for Standards (ISO) 27002 is a guideline of principles for initiating, implementing, maintaining, and improving information security management

(ISO, 2013). ISO 27002 provides a wide variety of security controls, including implementing a security policy, operational security, secure supplier relationships, and compliance (ISO, 2013). COBIT5 provides best practices for information security by defining functional responsibilities for information security, providing guidance for effective governance and management of information security, and providing best practices for linking information security to enterprise objectives (Information Systems Audit and Control Association [ISACA], 2012).

Security incidents and data breaches may occur from multiple threat vectors. In NIST's (2012a) Computer Security Incident and Handling Guide, several data loss vectors are described. Data loss vectors can come in many forms, for example, malware embedded on removable media that will infect a computer when launched, attacks by a disgruntled employee, malware loaded on a user's machine when he or she visits a web site with malicious code, malware embedded in an email, improper usage of data by a user, and loss or theft of equipment that holds sensitive data (NIST, 2012a). NIST suggests using the material in the Computer Security Incident and Handling Guide to prepare for security incidents, including a response if a security incident should occur. A plethora of best practices exist for financial services companies in protecting information and systems from data loss.

Summary

Heikkila (2009) suggested further research to understand how the use of IT may affect data security breaches. According to Verizon, in most of the breaches, there was a delay between the data breach and the discovery. Verizon reported that, in 54% of the data breaches, it took from one to 12 months from the time that the system was initially

compromised to the discovery of the data breach. The literature review explores research papers, reports by well-known technology vendors, government-supplied standards and policies, and news reports regarding data breaches. The collection of information provided in the literature review established there is a wide variety of threats and new information technologies that could lead to increased security threats, as well as multiple technologies providing new capabilities to security information and detect compromises.

Chapter 3

Methodology

This chapter presents the case study methodology that was used to investigate the research question proposed by Heikkila (2009), i.e., *Does information security technology correlate to increased prevalence of detecting a security breach?* This case study expanded on Heikkila's research question to include questions about the type of information technologies that may increase or decrease detection of security incidents and breaches. This chapter includes the research method employed; the case study research design, reliability, validity, and format for presenting the results, and the resources required. The chapter concludes with a summary.

Research Methods

The research method was a case study. According to Yin (2014), case studies contribute knowledge about groups and organizations and are the preferred method when (a) the research questions are “how” or “why,” (b) the researcher has little or no control over the behavior or event, and (c) the focus of the study is a contemporary phenomenon. This research focused on understanding how security incidents and breaches are affected by information technologies, such as data loss prevention, SIEM, IPS, MDM, and mobile container management. This research also investigated the reasons why a member of a Fortune 500 financial services company observes changes in the number of security incidents. The outcome of this investigation will contribute information to business and information security professionals who are tasked with protecting sensitive data.

Research Design

According to Yin (2014), case studies have five components: (a) research questions, (b) propositions, (c) units of analysis, (d) logic that links the data to the propositions, and (e) criteria for interpreting the findings. Yin defined research design as a logic plan to create the steps needed to bring a researcher from the original questions to the conclusions of the study. Research design addresses what questions to study, what data is relevant, what data to collect, and how to analyze the results (Yin, 2014).

Research Questions

RQ1: What type of information security products resulted in an increase detection of security incidents or breaches?

RQ2: What types of security information technology result in a decrease of security incidents and breaches?

RQ3: How have cloud and mobile technologies resulted in an increase or decrease in data security incidents and breaches?

RQ4: To what extent can participation in threat information sharing groups, or threat intelligence sharing, drive an increase or decrease in the number of security incidents and breaches?

Propositions

Yin (2014) identified the importance of describing propositions that are linked to research questions. According to Yin, propositions help the researcher to look for relevant evidence and reflect on the theoretical issue. In addition, case studies should be based on multiple sources (Yin, 2014). Table 1 presents the research questions, propositions, referenced sources, and planned interviews.

Table 1. Propositions

Proposition	Corresponding RQ	Source of Evidence	Reference Support
Proposition 1: SIEM and advanced persistent threat (APT) tools can detect attacks.	RQ1: What type of information security products resulted in an increase detection of security incidents or breaches?	Document review Interview	Cybenko & Landwehr, 2012; Gabriel, Hoppe, Pastwa, & Sowa, 2009
Proposition 2: SIEM and APT tools can increase the number of incident or breaches because the company becomes aware of more events.	RQ1: What type of information security products resulted in an increase detection of security incidents or breaches?	Document review Interview	Cybenko & Landwehr, 2012; Gabriel, Hoppe, Pastwa, & Sowa, 2009
Proposition 3: SIEM and APT tools can provide companies with methods to detect and stop an attack faster than before the tools were installed.	RQ1: What type of information security products resulted in an increase detection of security incidents or breaches?	Document review Interview	Cybenko & Landwehr, 2012; Gabriel, Hoppe, Pastwa, & Sowa, 2009; Lewis, 2013
Proposition 4: Information technology products exist that drive down the occurrences of data security incidents or breaches.	RQ2: What types of security information technology result in a decrease of security incidents and breaches?	Document review Interview	Alsuhibany, Morisset, & van Moorsel, 2013; Bau, Bursztein, Gupta, & Mitchell (2010); CyberArk, 2014; Lewis, 2013
Proposition 5: Utilizing new technologies increase the number of data security incidents and breaches.	RQ3: How have cloud and mobile technologies resulted in an increase or decrease in data security incidents and breaches?	Document review Interview	Kothari, 2013; Li & Clark, 2013

(Table continues)

Table 1 (Continued)

Proposition	Corresponding RQ	Source of Evidence	Reference Support
Proposition 6: Utilizing new information technology in concert with new information security defense technology protections reduces the likelihood of data security incidents and breaches.	RQ3: How have cloud and mobile technologies resulted in an increase or decrease in data security incidents and breaches?	Document review Interview	Kothari, 2013
Proposition 7: Utilizing threat sharing information provides a company a mechanism to reduce the number of data security incidents and breaches.	RQ4: To what extent can participation in threat information sharing groups, or threat intelligence information sharing, drive an increase or decrease in the number of security incidents and breaches?	Document review Interview	Lemos, 2013
Proposition 8: Utilizing threat sharing information without the security information technology to consume and defend against the threat will increase the awareness of data security incidents and breaches.	RQ4: To what extent can participation in threat information sharing groups, or threat intelligence information sharing, drive an increase or decrease in the number of security incidents and breaches?	Document review Interview	Moriarty, 2013; Ollmann, 2013

Unit of Analysis

Yin (2014) maintained that researchers should define the scope of the case, or the unit of analysis. For this study, the unit of analysis is Fortune 500 financial services companies. In addition, according to Yin, one of the most important sources of case study evidence is the interview, as it is expected to be more fluid than rigid. Yin suggested interview questions be phrased with *how* and *why* and that shorter case study interviews should last about an hour. The case study included interviews of nine Fortune 500 financial services security leaders. Due to the sensitivity of the topic, there were no recording of the interview sessions.

Linking Data to Propositions

According to Yin (2014), pattern matching is one of the most desirable techniques for case study analysis. Pattern matching involves comparing the findings from the case study with the predictive statements made before the researchers collect data (Yin, 2014). Yin indicated that the researcher should state the predicted propositions prior to the start of the investigation and compare the results to the original predictions; if the predicted patterns are similar to the results, the case study has stronger internal validity.

Findings Interpretation

According to Yin (2014), data triangulation strengthens the construct validity of a case study. In this analysis, the goal was to analyze multiple sources of data, such as documents, archival records, and interviews. This case study references multiple sources of evidence, including research papers, media stories, and technology papers published by technology vendors.

Reliability

Yin (2014) defined a case study protocol that the researcher should use to increase the reliability of the study. This protocol included developing case study questions and propositions, creating data collection questions, addressing rival explanations, maintaining a chain of evidence, and organizing documentation in a case study database.

A chain of evidence links the case study questions to the sources of data. When research data are stored in a case study database, linkages will be improved for use in a case study report, increasing reliability. The interviews of information security professionals in Fortune 500 financial services companies were anonymous. In the case study database, a chain of evidence was maintained to ensure that the data can be tied back to one specific, anonymous person representing a Fortune 500 financial services company.

According to Yin (2014), creating a case study database will help to organize the documentation and data collection and increase the reliability of the case study. The case study database typically includes interviews, tabular materials, observations, document analysis, and analysis of data.

Validity

Internal validity can be strengthened when a cause-effect link can be made, including showing the rejection of rival hypotheses (Yin, 2014). External validity relates to the extent that the findings of the case study can be analytically generalized to other situations (Yin, 2014). According to Yin, when empirical and predictive patterns appear to be similar, a case study's results can demonstrate stronger internal validity. Yin

suggests that, to improve external validity, the researcher replicate logic by using a multiple-case study design.

Yin (2014) defined construct validity as the accuracy in which a case study's measures reflect the concepts being studied. Yin suggested that, to increase construct validity, the researcher cite multiple sources of evidence, maintain a chain of evidence, and enable a review of the draft case study conclusions by key informants.

Format for Presenting Results

Yin (2014) identified multiple sections of a case study report. The researcher should (a) identify the research questions, (b) define the cases that will be studied, (c) connect the research question and the data, (d) consider rival conclusions, (e) describe how the data was collected, (f) explain the analysis methods used, (g) identify the sources of data, (h) explain any unexpected difficulties, (i) describe the method of analysis, and (j) identify any shortcomings of the design or analysis. Yin's outline was utilized, in addition to the Nova Southeastern University Dissertation Guide available for the Graduate School of Computer and Information Sciences (GSCIS) for doctoral students, for the case study report.

Resources Required

To complete the literature review, access to the online Nova Southeastern library as well as general Internet access was required, which provides a connection to the dissertation tracking system, guidelines for creating dissertations, general media articles, industry papers, and government documents. Many journal articles were referenced from MIS Quarterly, IEEE Security & Privacy, Computer Fraud & Security, and

Communications of the ACM. Vendor papers were referenced from IBM, Verizon, McAfee, CISCO, FireEye, and Symantec. Government documents were retrieved from the White House, NIST, CERT, HHS, SEC, and the U.S. Senate. From the Nova Southeastern electronic library, journal articles and dissertations were accessed.

The research benefited from the expertise of the dissertation chair and dissertation committee for overall direction and guidance. The dissertation chair reviewed the survey instrument (Appendix B). The Institution Review Board (IRB) processes were utilized to gain approval before conducting interviews.

Finding a set of security leaders from Fortune 500 financial services companies is difficult because companies avoid sharing sensitive information security data (Doherty & Fulford, 2005; Heikkila, 2009; Wiant, 2005). Existing relationships with financial services companies were utilized, where a level of trust had already been established with chief information security officers (CISOs) and managers who lead security teams. Data was anonymous and not tied back to a specific person or company, which increased the number of people who were willing to participate. Each interview and all associated data tied to that interview will be retained as a chain of evidence.

Summary

Heikkila (2009) suggested that research be done to understand how information technology corresponds to the prevention or reduction of security breaches. To understand how technology may correspond to a security incident or breach, a case study was performed of Fortune 500 financial services information security professionals. A case study was chosen to understand *how* security incident and breaches have changed and *why* the information security professionals at Fortune 500 companies believe they

have seen a change. Nine information security professionals of Fortune 500 financial services companies were targeted for an interview. Yin's (2014) pattern-matching approach for the case study analysis was utilized.

Chapter 4

Results

This chapter contains the results of the case study. It begins with a review of the goals, methodology, information gathered from the interviews, data analysis, and findings with regard to the propositions. The chapter concludes with a summary.

Review of the Methodology

The goal of this dissertation is to gain a deeper understanding on how information technology can increase awareness of a security incident or breach, and can also decrease security incidents and breaches. This dissertation also explores how threat information sharing increases awareness or decreases information security incidents and breaches. A case study was used as a research approach because case studies are a preferred method when (a) the research questions are “how” or “why,” (b) the researcher has little or no control over the behavior or event, and (c) the focus of the study is a contemporary phenomenon (Yin, 2014). Following Yin’s approach for case studies, documentation review and interviews were utilized to analyze the stated propositions. Interviews of Fortune 500 security leaders were a critical element of the study. Nine Fortune 500 financial services security leaders were interviewed. The participants were CISOs or managers within the information security teams. The job titles of the participants included Senior Vice President Chief Information Security Officer, Senior Vice President Information Technology, Vice President Chief Information Security Officer, and Chief Information Security Officer. All interview participants were men. All the participants were previous acquaintances through security industry conferences or meetings. All

interviews were performed over the phone and took an hour or less to complete. See Appendix B for the questions posed to the interview participants. Notes from the interview were and mailed the summary of the interview to the participant. Participants were offered to make any corrections to the transcribed answers. One participant provided a correction to the interview notes. A numbering scheme was utilized to represent each interview, but the notes did not contain the interviewer's name or company. A log of the names of all of the participants was retained including their mailing address, email address, and signed consent form. Postal mail was utilized to ensure maximum confidentiality of the participants. After the interviews were completed, each interview participant was mailed a summary of all the anonymous interview data. The study utilized pattern matching and explanation building when performing case study analysis, as defined by Yin (2014). Participants are referred to as A1 through A9. See Appendix C for the interview participant's responses.

Data Analysis

This section provides the research questions, propositions, and proposition findings.

RQ1: What type of information security products result in an increased detection of security incidents and breaches?

Proposition 1: SIEM and APT tools can detect attacks.

Proposition 2: SIEM and APT tools can increase the number of incidents or breaches because the company becomes aware of more events.

Proposition 3: SIEM and APT tools can provide companies with methods to detect and stop an attack faster than before the tools were installed.

Proposition 1 Finding: The responses from Interview Question 1A show that every company has been investing in SIEM, log management, or advanced network monitoring to understand APTs. The responses from Interview Questions 1B and 1C (see Appendix C) indicate that the companies were able to detect security incidents faster, with better correlation of multiple sources of data. Taking into account the interview data and triangulation of referenced material (Cybenko & Lanwehr, 2012; Gabriel et al., 2009), Proposition 1 was supported.

In addition to SIEM and APT tools, many other technologies were highlighted that provide greater detection of information security incidents. Some of the technologies mentioned were endpoint protection, which is able to detect malicious behavior; detecting malicious email; DDOS attacks; detecting large file transfers leaving the company; having a service provider scan the network for Indicators of Compromise (IOCs); decrypting network traffic that leaves the enterprise to interrogate for malicious activities; and detecting communication to malicious websites.

Eight out of the nine interviewees mentioned they were monitoring their company network to increase awareness of security incidents and breaches. Four of the nine interviewees mentioned using information technology to detect malicious code on the endpoint to increase awareness of security incidents and breaches. Two of the nine participants mentioned the use of DLP to detect security incidents and breaches. Some approaches were only mentioned by one interviewee. Interviewee A2 identified the use of monitoring active directory access rights. Interviewee A4 identified decrypting network traffic to interrogate the contents of the communications. Interview participant A2 identified the use of next generation firewalls as a key technology to increase awareness

of security incidents and breaches. Next generation firewalls provide a deeper inspection of data entering or traversing the network, with the ability to reroute or block network traffic. Both A2 and A4 identified the use of monitoring directory permission changes. Utilizing this technology, the interview participants were able to detect if a hacker or malicious insider was altering access rights to implement an attack on the system. Interview participant A4 identified the approach of decrypting and interrogating network traffic to look for malicious activities. Malicious actors can utilize encryption to hide data exfiltration from the network. Bluecoat's SSL visibility appliance (2015) is an example of a solution that unencrypts SSL traffic so a company can gain visibility into data leaving the network. Encryption can create a blind spot for advanced malware (Bluecoat, 2015). Interview participants A7 and A9 identified the importance of employees identifying SPAM, and how the security teams utilized the information to search for IOCs. The answers demonstrate the connection of people, process, and technology to detect security incidents and breaches.

A5 and A8 mentioned utilizing professional services, where the service provider brought in their own tools to detect security issues. Utilizing professional services to bring in unique tools, allowed the interview participants to gain insight into their networks without buying and installing new security information technology. Interview participants changed service providers every year, with the belief that this approach provided the chance for finding exposures that might have been missed by the other service provider. A7 identified monitoring cloud services to ensure the use of the cloud service was authorized by the company.

Future research could explore the effectiveness of these technologies. A possible weakness in the study is that the interview question asked the participants to focus on technology installed within the last three years. Without a complete inventory of technology installed, commonality or differences could be missed. Future research could compare the total inventory of security products installed, and their effectiveness. The interview data exposes many other security technologies that provide increased detection of an attack in addition to SIEM and APT tools. Some examples are detecting large file transfers leaving the company network. A short coming of the research design was the narrow proposition, but the questions provided a means to gain a richer set of answers from the participants.

Proposition 2 Finding: Proposition 2 suggests that SIEM and APT tools cause an increase in the detection of data security incidents and breaches. Using the responses from Interview Question 1D, and triangulating with referenced material (Cybenko & Lanwehr, 2012; Gabriel et al., 2009), Proposition 2 was supported. The interviews identified several similar answers, where participants highlighted that, without the security detection technology, they would have been blind to the security threat.

Interviewees A1 and A7 highlighted that they are detecting increased threats and have larger attack surfaces to protect. Both A2 and A9 mentioned that they measured the effectiveness of new security information technology, and could demonstrate improvements in decreased security incidents and improved penetration results. A3 identified that DLP provided insights into broken business processes, ultimately decreasing security incidents and breaches once addressed. What is striking is the multiple ways that the participants described their increased awareness of security

incidents and breaches. Words like visibility, insights, awareness, and seeing more details were used. Many of the interview participants described that the technology allowed them to react quicker by using words like quarantined and isolated faster, detected earlier in the attack, detected and stopped attack, and detected information quicker. Participant A7 identified that additional staff was needed to analyze the data provided by the security technology.

A possible short coming of the research design, and future research opportunity is to explore in more depth how increased awareness of security incidents and breaches led to improved security for the enterprise. Utilizing answers from A2 and A9, we know data exists that increased awareness of security incidents and breaches can lead to improved security, because A2 and A4 had metrics to support their improvements. The information security identified by the interview participants spanned many other technologies in addition to SIEM and APT tools.

Proposition 3 Finding: Proposition 3 suggests that information security products can detect and stop security threats. Using triangulation of interview data and referenced material (Cybenko & Lanwehr, 2012; Gabriel et al., 2009; Lewis, 2013), Proposition 3 was supported. The results of Interview Questions 1D and 1E show that the participants were consistent in highlighting that technology gave their teams the ability to detect a threat earlier in the attack cycle and stop the threat. Five out of the nine interviewees mentioned that the information technology they have installed in the last three years has provided their teams increased ability to detect and react to a threat quicker. Six of the nine participants stated that new security information technology pointed out security threats that in the past they would have been unaware. The participants used many ways

to describe how they detected and stopped security threats. Some examples where they would not have found the compromise without the new technology, and that without the new technology they would have been oblivious of the attack. Without the new technology they would have caught the compromise much later in the attack cycle. An interview participant identified the use of information technology that could identify what “normal” network traffic was and monitor for “not normal”. This technology capability allows the company to possibly detect a hacker taking over a user’s access.

RQ2: What types of security information technology result in a decrease of security incidents and breaches?

Proposition 4: Information technology products exist that drive down the occurrences of data security incidents and breaches.

Proposition 4 Finding: Proposition 4 states information technology products exist that can decrease the occurrence of data security incidents and breaches. Utilizing the interview data and referenced material (Alsuhibany et al., 2013; Bau et al., 2010; CyberArk, 2014; Lewis, 2013), Proposition 4 was supported. The participants identified multiple IT security capabilities that decreased the occurrence of data security incidents. The prevention technologies mentioned most often were blocking malicious web sites, DLP, and application whitelisting. Other technologies highlighted were patching the infrastructure, blocking command and control servers, privileged user management, host IPSs, phishing programs, vulnerability scanning, and SPAM filtering.

The participants believed they experienced fewer security incidents because these technical capabilities reduced the amount of malware entering their systems, and the technology pointed out processes that could be enhanced to improve security. Two of the

nine participants specifically mentioned their new technology decreased malware infections entering their systems through email. Analyzing answers from both questions 2D and 2E, almost every participant mentioned that new security information technology allowed their teams to react faster. One participant highlighted specific security technology that identified application code vulnerabilities, and had provided data that helped facilitate conversations with application code developers, leading to improved code development. Three of the nine participants interviewed mentioned new information security technology identified broken processes they were able to address. Some participants mentioned technology that was not repeated consistently by other participants. Examples of some unique technologies mentioned were whitelisting, next-generation firewalls, and application vulnerability scanning.

Reflecting on the interview data from Question 2, many of the same technologies that were also mentioned in Question 1. It could be concluded that the same technology that provided greater awareness of security incidents and breaches also provided a mechanism to decrease security incidents and breaches. Examples were dissecting SSL traffic to look for malicious traffic, next generation firewalls, identifying anomalous behaviors, and application vulnerability scanning. The interview participants had a focus on security technology that could prevent malware, including patching, blocking websites, and preventing applications from being exploitable by hackers. One interview participant mentioned improved patching multiple times. Patching is not an advanced technology, but is a foundational element in information security. There was a theme of activities that interview participants mentioned. The participants were focused on decreasing malware through patching, blocking malicious websites, and eliminating malicious SPAM. The

participants decreased the chance of security incidents and breaches by hosting application code with less security vulnerabilities. Security technology was used for increased awareness of security incidents and breaches, and decreasing security incidents and breaches.

Without a complete list of technologies each company is using, there is a possibility of more commonality than was extracted from the interviews. Future research could track the improvements in the amount of time to detect and remediate a security incident or breach.

RQ3: How have new technologies, for example, cloud and mobile technologies, resulted in an increase or decrease in data security incidents and breaches, and has the technology strengthened or weakened enterprise security?

Proposition 5: Utilizing new technologies increases the number of data security incidents and breaches.

Proposition 6: Utilizing new information technology in concert with new information security defense technology protections reduces the likelihood of data security incidents and breaches.

Proposition 5 Finding: Proposition 5 states that utilizing new technologies increases the number of data security incidents and breaches. Utilizing the answers from Interview Question 3B, Proposition 5 was not supported. The majority of the respondents did not see an increase in the risk of using cloud services or mobile devices. In almost every interview, the participants identified increased usage with mobile devices. Usage spanned from limited use of mobile for email, calendar, and contacts to support of many mobile applications. In almost all cases, participants highlighted the increased use of the cloud,

but again the answers spanned from no use of cloud to a business decision to consider cloud first. The participants did not identify any situations that created a security incident or breach using cloud technology, and only one security incident on the mobile platform. Analyzing the interview responses, it is striking the variety of utilization of mobile and cloud technologies, resulting in a consistent view that there have been no or isolated security incidents and breaches on mobile devices and cloud services. The use of mobile devices included the support of employee owned without company MDM management, to strongly managed devices with MDM and containerization. Only one interview participant mentioned a mobile malware infection on the Android platform. Cloud usage spanned from no use of cloud services to choosing cloud as the first choice as a hosting platform. . One interview participant believed the risk of a security incident or breach increased, but that there was no data to support that belief. Future research could consider the differences of incidents and breaches between different financial services companies that have avoided the use of cloud services to companies that consider cloud services as their first choice as a hosting platform.

Proposition 6 Finding: Proposition 6 states that utilizing new security technology to address expanded information technology reduces the likelihood of data security incidents and breaches. Proposition 6 was supported because the participants identified that, in some cases, cloud and mobile technology provided better security for a specific use. Alternatively, in every case, interview participants had identified technology used to secure both mobile and external cloud environments. The participants identified several pieces of technology that they utilized to improve the security of new enterprise technology. Almost every participant mentioned the use of MDM and containerization to

secure mobile devices. When asked about the increased risk of expanded use of mobile devices, most participants did not see any increased risk. Only one participant identified increased security incidents or breaches related to the mobile or cloud platform. To protect against security incidents and breaches when using cloud services, the participants mentioned utilizing data encryption and monitoring usage of cloud services so that employees would be limited to using public cloud services that were approved by information security.

Utilizing the interview data, the study determined that several participants viewed the external cloud environment as more secure than their internal infrastructure. Participants mentioned that the external cloud services environment were less complex and more locked down than was their internal infrastructure. The concerns the interview participants raised was ensuring the company utilized only security-vetted cloud services and enforcement of a secure design when using the authorized cloud service. The participants described their use of information technology and processes to ensure that employees were using only sanctioned cloud services. Participants were not consistent in their view of risk related to the cloud platform. Feedback from the interview related to comparing the security of an on premise solution to a cloud solution ranged from weaker to more robust. As more workloads move to the cloud in both software-as-a-service and infrastructure-as-a-service model, there is an opportunity for additional research relating to the security differences of alternate cloud offerings. None of the participants mentioned experiencing any security incidents or breaches on cloud platforms, to date, and only one mobile malware incident. Future research could reconsider this research

question, if there are future major breaches with popular cloud service providers or mobile platforms.

In interview question 3C, participant A8 mentioned the use of virtualization as a technology to decrease security incidents. Future research could focus on the effectiveness of utilizing virtualization technology to secure an enterprise.

RQ4: To what extent can participation in threat-information sharing groups, or threat intelligence information sharing, increase awareness of security incidents and breaches?

Proposition 7: Utilizing threat sharing information provides a company a mechanism to reduce the number of data security incidents and breaches.

Proposition 8: Utilizing threat sharing information increases awareness of security incidents and breaches.

Proposition 7 Finding: Proposition 7 states that utilizing threat-sharing information reduces the number of security incidents and breaches. Proposition 7 was supported by several interview responses. All the participants interviewed were member of FS-ISAC, and several participated in additional threat-sharing organizations. The interview participants provided limited examples of where their participation in threat-sharing forums was tied to preventing specific incidents and breaches. The information that FS-ISAC provided to member companies with respect to the DDOS attacks against financial services companies was the only example given of an avoided security incident, which multiple interview participants mentioned. Several interview participants mentioned the DDOS example as a specific piece of information they utilized that reduced their security incidents. In general, there was a consistent theme from several participants, i.e., that the amount of information provided by FS-ISAC was too hard to consume and not specific

enough to avoid a targeted cyber attack. Some participants were trying to automate ingestion of threat information. Analyzing the participant interview data, it is striking the variety of answers. Many interview participants seemed overwhelmed with the data received from FS-ISAC. The value of FS-ISAC that was highlighted was the professional exchange with other members, information about wire transfer scams, and the ability to utilize information shared about cyber threat trends with the business. To gain the most out of FS-ISAC may require more involvement with FS-ISAC than ingesting the daily information bulletins.

Four of the nine participants identified intelligence related to DDOS attacks was very useful in decreasing the likelihood of a security incident. One of nine participants identified specific intelligence related to their involvement around a public event was very useful in avoiding a security incident.

Proposition 8 Finding: Proposition 8 suggests that utilizing threat-sharing information will increase awareness of security incidents and breaches. Proposition 8 was not consistently supported by a majority of participants interviewed. In one interview A4 identified a situation where they utilized threat information to avoid a security incident, specifically, very actionable intelligence related to a public event the company was involved. Multiple participants identified intelligence assisted them with defending against DDOS attacks. It is possible that, after applying the threat intelligence information to an institution's security infrastructure, the company was unaware of how that new control prevented a security incident or breach. Considering the focus of threat information sharing by the US Government, it is surprising the lack of examples about the effectiveness of threat intelligence ingested.

Table 2 presents a summary of the information regarding the propositions. It includes the proposition's corresponding research question and whether or not the proposition was supported.

Table 2. Summary of Results

Proposition	Corresponding RQ	Results
Proposition 1: SIEM and APT tools can detect attacks.	RQ1: What types of information security products result in an increased detection of security incidents and breaches?	Interview participants and other reference material supported the proposition.
Proposition 2: SIEM and APT tools can increase the number of incidents or breaches because the company becomes aware of more events.	RQ1: What types of information security products result in an increased detection of security incidents and breaches?	Interview participants and other reference material supported the proposition.
Proposition 3: SIEM and APT tools can provide companies with methods to detect and stop an attack faster than before the tools were installed.	RQ1: What types of information security products result in an increased detection of security incidents and breaches?	Interview participants and other reference material supported the proposition.
Proposition 4: Information technology products exist that drive down the occurrences of data security incidents and breaches.	RQ2: What types of security information technology result in a decrease of security incidents and breaches?	Interview participants and other reference material supported the proposition.
Proposition 5: Utilizing new technologies increase the number of data security incidents and breaches.	RQ3: How have cloud and mobile technologies resulted in changes to the frequency of data security incidents and breaches, and has the technology strengthened or weakened enterprise security?	Information collected from interview participants did not support the proposition
Proposition 6: Utilizing new information technology in concert with new information security defense technology protections reduces the likelihood of data security incidents and breaches.	RQ3: How have new technologies, for example, cloud and mobile technologies, resulted in changes to the frequency of data security incidents and breaches, and has the technology strengthened or weakened enterprise security?	Information collected from interview participants supported the proposition.

(Table continues)

Table 2 (Continued)

Proposition	Corresponding RQ	Results
Proposition 7: Utilizing threat sharing information provides a company a mechanism to reduce the number of data security incidents and breaches.	RQ4: To what extent can participation in threat-information sharing groups, or threat intelligence information sharing, increase awareness of security incidents and breaches?	Interview participants and other reference material supported the proposition.
Proposition 8: Utilizing threat sharing information increases awareness of security incident and breaches.	RQ4: To what extent can participation in threat-information sharing groups, or threat intelligence information sharing, increase awareness of security incidents and breaches?	Information collected from interview participants was not consistent in the support of the proposition.

Summary of Results

When the interview participants were describing the technology they installed to increase awareness and detect a security incident or breach, compared to the technology they installed to prevent a security incident or breach, the proportional level of effort that the interview participants described as being applied to detection capabilities compared to preventive capabilities was striking. Analyzing the interview data and factoring in the discussion, it was observed that Fortune 500 financial services companies identified about twice as many examples of detection vs. prevention technologies utilized in the past three years. Many of the participants stated that, without the new technology, they either would have never found the security issue or would have found it much later in the attack cycle.

There was a lack of incidents and breaches mentioned by the interview participants on mobile platforms. The interview participants seemed confident in the technology that they applied to secure mobile devices. An alternate explanation to the lack of incidents is that the participants interviewed may not be aware of a security incident on their mobile devices. According to McAfee (McAfee Labs, 2015), mobile malware has increased 50% in the first half of 2015 compared to 2014. McAfee suggests that mobile malware is in the early stages of effectiveness, and to date the malware has not been serious or broad based. The security of mobile devices could be reconsidered if serious, broad-based attacks materialize.

The majority of the interview participants considered vetted cloud service providers to be more secure than their internal IT infrastructure. Financial services companies are highly regulated, so the position that cloud services are highly secure is noteworthy. An

interview participant stated that the lack of visibility into security issues regarding cloud services was a concern. There was a question as to whether the external cloud services are as secure as the interview participants believe they are, or if the participants are informed of security issues the cloud service providers may have.

Considering the proposed legislation to increase threat sharing between the U.S. government and the private sector (U.S. Congress, 2015), it was surprising that almost every participant interviewed seemed overwhelmed with the amount of threat information received through FS-ISAC and struggled to identify specific situations the threat information provided to prevent a security incident or breach. One possible explanation is that the individuals interviewed were CISOs or senior information security leaders within their company and it is possible that someone on their staff was dealing with the threat intelligence and the interview participants were unaware of the specific incidents the daily threat information was preventing.

Chapter 5

Conclusions, Implications, Recommendations, and Summary

This chapter provides the conclusions of this study, along with limitations and recommendations for future areas of research. The chapter concludes with a summary.

Conclusions

The purpose of this study was to explore how IT security related to the prevalence of detecting a security incident or breach. Heikkila's (2009) dissertation focused on studying the relationship between the existence of a security policy and the proposition that a security policy could lead to decreased security incidents and breaches. Her dissertation did not find a statistically significant relationship between these two variables. Heikkila observed that, in some cases, newer IT security provided increased awareness of security incidents and breaches. Heikkila suggested further research to explore the relationship of IT security to increased detection of security incidents and breaches.

The first research question in this study explored whether IT security provided increased awareness of security incidents and breaches. Using triangulation, as described by Yin (2014), along with referenced material and interviews with nine leaders of information security in Fortune 500 financial service companies, the case study determined that IT security can increase detection of security incidents and breaches and strengthen enterprise information security. Interview participants highlighted SIEM technology, technology to scan infrastructure for IOCs, and advanced endpoint technology to identify anomalous behavior as some of these technologies used to identify security incidents they would have been unaware of in the past.

Cybenko and Landwehr (2012) noted the difference between information security and other safety programs, for example, automobile safety. With automobile safety, prior to 2012 there was not much change, but with information security, there are constant changes by attackers, defenders, vendors, policymakers, and decision makers. Cybenko and Landwehr proposed that SIEM is a necessary ingredient to defend against attackers. To address the full spectrum of adversaries, SIEM consolidates large amounts of security event data that spans multiple systems. Use of SIEM technology could lead institutions to discover security incidents of which they were previously unaware (Gabriel, Hoppe, Pastwa, & Sowa, 2009). SIEM technology allows companies to interpret security log data from network logs and access control information. Lewis (2013) explained that a SIEM tool cannot stop an attack, but the technology allows an institution to contain the attack and mitigate the possible damages by identifying the threat and taking action before the attacker becomes entrenched in their network. According to Verizon (2013), most of the breaches experienced a delay between the data breach and its discovery. Verizon reported that breaches may take months or years to discover and that, in most cases, third parties discovered the breaches.

The second research question explored what security technology was used to decrease security incidents and breaches. Utilizing triangulation of referenced material and interviews with security leaders working for financial services companies, the case study concluded that recently installed security technology decreased security incidents and breaches. Multiple companies have seen decreases in security incidents and breaches with technologies, including blocking malicious web sites, DLP, and application

whitelisting. The security technologies mentioned by the interview participants reduced malware infections, thereby decreasing security incidents and breaches.

IT security provides protection of informational assets for companies. Examples of IT security are access controls, endpoint controls, network controls, and host controls. Lewis (2012) suggested that companies deploy solutions that control privileged user accounts by auditing and logging all activities. CyberArk (2014) claims that misuse of privileged accounts, that provide elevated access rights, represent the largest security vulnerability that organizations have. Privileged users have elevated administrator access to systems, but this elevated access in the hands of a malicious user or hacker could alter IT infrastructure, disable security controls, steal information, and commit financial fraud (CyberArk, 2014; NetIQ, 2015).

To address threats related to privileged users, products like CyberArk and NetIQ provide a method to store privileged users' passwords in a vault and allow a policy to be defined to identify who can access the passwords and under what circumstances. Privileged user management products monitor privileged user sessions, can record a privileged user's actions, and have the ability to detect malicious activity by privileged users. Companies also can eliminate hard-coded passwords in applications using privileged user management technology. Taking into account privileged user management product claims, security incidents could decrease.

Researchers are looking for ways to detect internal attacks. Alsuhibany, Morisset, and van Moorsel (2013) developed a model called Attacker Learning Curve to monitor privileged users who are engaging in malicious activities. The model records attempts to access computer resources that utilize an unsupervised learning algorithm.

Bau, Bursztein, Gupta, and Mitchell (2010) studied existing black-box application vulnerability testing solutions to identify opportunities for improved capabilities to locate security vulnerabilities in applications. Bau et al. reported that there are over 50 products commercially available to scan and identify application vulnerabilities that are approved by the PCI-DSS council. The PCI-DSS council is an open global forum launched in 2006 that leads the development, management, education, and awareness of the Payment Card Industry Security Standard. The five founding members are American Express, Discover, JCB International, MasterCard, and Visa (PCI Security Standards Council, 2006).

Nair, Drew, and Verderber (2009) identified the requirement to analyze applications for security vulnerabilities. The highest risks are applications that are exposed externally, where users and hackers outside the company have access to the application. These applications are referred to as web facing (Nair et al., 2009). Eliminating application vulnerabilities of web-facing applications can decrease a company's risk of cyber attack (IBM, 2014a) as well as decrease the opportunity for a security incident by reducing application vulnerabilities for hackers to exploit.

The third research question provided insights into understanding how new and expanding use of IT related to security incidents and breaches. The interview questions focused on the expanded use of mobile devices and the use of cloud services. Surprisingly, none of the interview participants mentioned any security incidents and breaches related to mobile computing or the use of cloud services. In almost every interview, the participants explained how they utilized MDM and containerization technology to ensure the security controls and the data protection on the mobile device.

The Verizon breach report (2015) indicated that out of the tens of millions of mobile devices, only 0.03% of the devices had malicious exploits.

The majority of the interview participants viewed external cloud services as more secure than their internal infrastructure. A common theme was that the participants did extensive reviews of external cloud service providers, and companies sanctioned and controlled communication to only approved cloud service providers. Several participants indicated they used information security technology to monitor and prevent connections to unauthorized cloud service providers.

For those interview participants who considered external cloud services more secure than internal infrastructure, many believed that one of the reasons external cloud services were more secure was the simplicity of the cloud service vs. the complexity of their internal infrastructure. Based on the interviews, mobile technology and cloud services did not seem to increase security incidents and breaches. The lack of increased security incidents in the mobile and cloud space could be related to two reasons. One reason, several interview participants mentioned, was the lack of visibility into the cloud services infrastructure. A security incident or breach could be occurring at the cloud service provider, and the company might be unaware of it. The second reason there may be a lack of security incidents is that the companies interviewed utilized multiple information technologies to decrease their risk of information security incidents and breaches in the cloud. Examples of IT security utilized were encryption, and controls on usage of external cloud services. One interview participant indicated they did not utilize any cloud services.

Kothari (2013) explained that cloud technologies carry increased risk, especially for financial companies that hold large amounts of regulated data, such as bank account numbers, social security numbers, and health information. NIST (2010) defines personal identifiable information (PII) as information that, if exposed, could cause negative impact to a person. Examples of PII, as defined by NIST, are passport numbers, driver license numbers, social security numbers, financial information, and biometric data. To combat the increased risk when using cloud technologies, Kothari (2013) suggested encrypting user data both in transit and at rest; retaining encryption keys; deploying DLP techniques, such as software that looks for specific keywords; and utilizing malware detection techniques, such as anti-virus software and intrusion prevention systems. Encryption of company data and retention of the encryption keys are important because cloud providers may have access to the data. If the data are encrypted, the information will not be able to be deciphered by the cloud service provider, provided that the cloud service provider does not have access to the encryption keys. Companies that use cloud services need to be aware of the location of the data to ensure that privacy laws are being complied with when data are being transported across country boundaries (Kothari, 2013).

Mobile computing continues to grow and creates additional security threats that need to be considered. Mobile applications are often inexpensive and easy to buy (Li & Clark, 2013) but are vulnerable to malware or to a hacker's gaining access by rooting or jailbreaking the device (bypassing the device's security controls; Li & Clark, 2013). Mobile security products exist to provide content containers to separate personal and business data, monitor the security health of the device, and provide secure encrypted email. A few of the companies that provide security products for mobile devices are

Good (2014) and AirWatch (2014). Lookout is an anti-virus vendor for Android mobile devices (Lookout, 2014). Trend Micro Mobile Device Security blocks phishing and malicious websites for iPhones and iPads (Trend Micro, 2015). However, even with additional security technology, threats exist. German security researcher Andreas Kurtz discovered a flaw with the Apple iPhone and iPad that allows the hacker to bypass the security controls and obtain access to email attachments (Pagliery, 2014). Even though this vulnerability has since been fixed by Apple, it is an example of the ongoing challenge researchers and hackers take on to search for product vulnerabilities.

The last research question concerned the effectiveness of threat-sharing forums. All interview participants were members of FS-ISAC, and many identified additional threat-sharing forums they were involved in. Surprisingly, there were consistent comments from the interview participants on the limited value of threat-sharing forums. There was only one interview participant who identified a specific targeted situation in which the information provided by FS-ISAC prevented an attack. Four of the nine participants identified intelligence around DDOS attacks helped them prevent a security incident. There was a consistent theme that the information from FS-ISAC was a huge amount of data, and their companies struggled to consume the information.

The feedback from the nine Fortune 500 financial services individuals interviewed indicated that there was a question regarding the effectiveness of the Cybersecurity Information Sharing Act of 2015, passed by Congress (U.S. Congress, 2015). A requirement of the cybersecurity legislation is to request the Department of Homeland Security develop procedures to share cybersecurity threat information with private entities. A few of the interview participants indicated they were in the early

implementation stage of automated updating of threat indicators into their enterprise security systems; future research could explore the readiness of different industries to intake threat indicators. FS-ISAC is a leader in working to solve the issue of consuming large amounts of threat information and has partnered with DTCC to create a new company with a mission to provide automation and services to aid the automatic updating of threat information into existing security controls (Soltra, 2015).

Threat intelligence services provide information about attackers and their methods of hacking (Wilson, 2013). The exchange of threat information among and between financial services companies through FS-ISAC (2013a) and government agencies may have the potential to affect the number of incidents or breaches. There are multiple groups that share threat information. FS-ISAC requires financial services companies to join FS-ISAC, by paying a membership fee, to gain access to the information. The cost of the membership is a sliding scale, depending on the services bought and the size of the financial institution.

Free threat-information sharing services are used to gain knowledge of security threats. The U.S. CERT (2014) provides information free of charge to companies and individuals. InfraGard (2015) is a free service that the FBI provides after the applicant is vetted. InfraGard has over 80 chapters and serves 16 critical infrastructure segments. Threat information also can be integrated with security information and event management solutions (Lemos, 2013). Intelligence sharing and acting on the intelligence are important to combating cyber threats (Mandiant, 2013).

Strengths

The high response rate was the strength of this study. Although there were nine interview participants, two additional individuals refused to participate because their company policy prohibited signing the consent form. Two other individuals agreed to participate and provided signed consent forms, but they could not make time in their scheduled to be interviewed. There is a general reluctance to participate in information security research, which leads to typical low response rates to security research, unless there is an established relationship with the surveyed organizations. For example, Heikkila (2009) distributed a Web-based survey to 1,123 Information Legal Technology Association members and received 88 valid responses, a 7.83% valid response rate. The research by Doherty and Fulford (2005) surveyed 2,838 people, with a 7.7% valid response rate. Wiant (2005) surveyed 2,500 people, with a 5.6% response rate. Finding willing participants was an integral part of this research.

Within a week of the interview, notes from the interview were transcribed and mailed them to each participant. Interview participants were instructions to provide feedback if they would like any corrections or changes made. One correction was received from an interview participant. The participants interviewed were involved in conferences or events where introductions happened, which may indicate some shared interest or profile.

Weaknesses

There could be a bias on the part of the author or the participants. Interactions with the interview participants existed prior to the interviews. The interaction spanned from one prior interaction to many interactions over several years. There is also a possibility of participant bias, as the participants were approached at an external activity (outside the

company) in which both parties were involved. There is a possibility that Fortune 500 financial services companies that were not approached could have a different point of view, not captured in the case study results. Because there was some interaction with every participant prior to the interview, there could have been bias in the design of the questions, the method of interviewing, or the recording of answers.

Limitations

The results of this case study may have limited applicability to other populations, as the financial services industry is highly regulated. In addition, the levels of information security regulations are different across industry segments; thus, the results from this case study may be different in other industry segments. Further, the participants in this study were from the financial services sector, but none were from the top 20 Fortune 500 companies. There is a possibility that the largest financial sector companies could have a different perspective than was captured in this case study.

Implications and Recommendations

Many regulations are focused on the reporting of data breaches (Mintz Levin, 2015; National Conference of State Legislators, 2013; Singer, 2013; Stevens, 2012; U.S. Department of HHS, 2013b). Proposed legislation is focused on more aggressive sharing of IOCs by the U.S. government with the private sector. This case study may lead to further research, such as whether companies should be viewed more positively by regulators when a company has a solid security program and a reputation for finding and responding to security incidents or breaches. Should quickly finding and resolving a

security incident or breach be viewed more positively than being informed by a 3rd party that a breach has occurred?

Financial services companies have a highly mature ISAC in which to participate. The participants consistently highlighted that keeping up with the FS-ISAC threat intelligence feeds was challenging. FS-ISAC and the DTCC are working to develop more automated methods to consume the threat intelligence feeds. Additional research could explore whether the government needs to focus on the ability of companies to effectively utilize threat feed information in addition to improving the sharing of IOCs and threat information. Research also could be conducted to determine the effectiveness of automated consumption of threat information. Further, as this study was focused on the financial services sector, future research could consider other industry sectors and their associated ISACs.

The Fortune 500 financial services interview participants were CISOs or information security leaders in their companies. It is possible that there is a different perspective on the applicability of threat intelligence information to prevent or stop a security breach, namely, from the technical team who consume the daily threat intelligence feeds. Future research could study the perspectives of technical security team leaders, for example, security operations center managers.

This case study had the participants focus on the last three years of new investments. Future research could consider the total inventory of security technology utilized. The focus on detection vs. prevention information security technology may show a different balance of investment and focus if the entire set of capabilities were considered.

Several of the interview participants indicated they considered vetted and approved cloud service to be more secure than their internal infrastructure because the cloud service provider's security capabilities were robust, and the security architecture was less complex than their internal infrastructure. Most of the participants were new to utilizing cloud services. Future research could consider how information security risk changes as companies grow their utilization of cloud services, as well as how resilient the corporate enterprise is as multiple cloud services providers are used.

Cadregari and Cutaia (2011) identified some of the security risks related to cloud technology to be data protection, data disposal, physical controls, access controls, logical controls, and reporting obligations. This research focused on the increase or decrease of the detection of security incidents and breaches related to utilizing cloud services. Future research could explore the perceived strength or weakness of cloud services to internal infrastructure relating to data protection, data disposal, physical controls, access controls, logical controls, and reporting obligations.

Miyamoto (2013) identified people as the weakest link in information security. Several interview participants identified their security staff as critical in identifying a security issue or breach that technology missed. Future research could analyze the type of security incidents that are missed by technology and detected by humans. Another future research opportunity could explore what skills security professionals need for a greater likelihood of finding security incidents that technology misses. Another possible research topic could be to study the necessary staffing levels and time spent to look for security anomalies to effectively find security incidents for a specific industry sector.

Summary of the Study

Cyber security is a major focus of the government and companies today. Results from a survey conducted by PwC (2015) on the state of information security showed that there was a 38% increase in the security incidents detected, while information security budgets grew by 24% in 2015 as compared to 2014. The U.S. Congress passed a cyber security bill that requires more aggressive cyber intelligence information to be shared between the government and private sector (U.S. Congress, 2015). U.S. government regulators, for example, the FFIEC (2015b), are holding board of directors responsible for the cyber security capabilities of the institutions they oversee.

This case study explored the information security technology related to an increased awareness and a decrease in information security incidents and breaches focused specifically on the financial services industry. The research also explored the case study participants' views of threat indicator sharing. This research could provide companies, government agencies, and ISACs with insights into the perspectives and challenges of Fortune 500 financial services information security leaders, as companies address the challenges of improving information security capabilities and reducing the possibility of an information security breach.

Wiant (2005), Doherty and Fulford (2005), and Heikkila (2009) explored the relationship between security policies and data security breaches, and the findings of all three investigations demonstrated that there was no statistically significant relationship between having a security policy and realizing a reduction in data security breaches. The goal of this study, however, was to look at the increase or decrease of security information and breaches from the perspective of IT and not the existence of a security

policy. Heikkila observed in her dissertation that some of the firms with increased detection of security breaches had superior information security technology. She suggested further research to explore how IT security corresponded to an increased awareness of security incidents and breaches. This case study expanded on Heikkila's proposal for further research by considering four research questions:

RQ 1: What type of information security products result in an increased detection of security incidents and breaches?

RQ 2: What types of security information technology result in a decrease of security incidents and breaches?

RQ 3: How have new technologies, for example, cloud and mobile technologies, resulted in an increase or decrease in data security incidents and breaches, and has the technology strengthened or weakened enterprise security?

RQ 4: To what extent can participation in threat-information sharing groups, or threat intelligence information sharing, increase awareness of security incidents and breaches?

This research topic was very relevant over the course of the study. Breaches continued to occur, making major media headlines. Some noteworthy breaches in 2015 included Anthem's loss of 80 million records, CareFirst Blue Cross Blue Shield's breach of 1.1 million records, Premera's breach of 11 million records, Excellus Blue Cross Blue Shield's loss of 10 million records, the Experian breach of 15 million records, ScottTrade's breach of 4.5 million records, the IRS breach of over 700,000 individuals' records, and the U.S. Office of Personal Management's breach of 21.5 million records (Privacy Rights Clearinghouse, 2015).

Insurance, financial, and government sectors experienced major breaches in 2015. Ironically, information security breaches grew as spending on information security increased (PwC, 2015). The U.S. government advanced cyber security legislation, looking for ways to improve the cyber security capabilities of the country. In 2013, President Obama signed an executive order aimed at improving the country's cyber readiness (White House, 2013). Part of the executive order tasked NIST with producing a new standard for critical infrastructure to improve the cyber protections of companies (NIST, 2014a). Congress also passed a cyber security bill that required more aggressive cyber intelligence information sharing between the government and private sector (U.S. Congress, 2015).

Continued breaches and increased government oversight demonstrated the lack of any specific solution to eliminate information security breaches. This research focused on providing insight into how financial services information security leaders viewed IT and threat intelligence sharing as tools to provide increased awareness and decrease information security incidents and breaches. Nine information security leaders of Fortune 500 financial services companies were interviewed. Interviews lasted approximately one hour. Notes were recorded from the interview and provided a record of the notes to the participants, allowing them to suggest any changes or corrections. Using Yin's (2014) guidance on case study research, pattern matching and triangulation were utilized to provide findings. Plausible rival explanations were explored.

The case study revealed several insights. Using pattern matching, the study discovered that there were consistent responses with regard to security technology that had been installed in the last three years to provide companies with increased awareness

of data security incidents and breaches. Several participants stated the new technology had improved their visibility of security incidents and breaches from months and years to hours and days. There was a consistent view that, without the newer detection capabilities they installed, in many cases, the company would have been unaware of the security incident. The most referenced detection technologies mentioned were SIEM, log correlation, and malware detection. The interview participants also saw a decrease in security incidents and breaches from information security technology that provided prevention capabilities. The technology mentioned most often was blocking malicious web sites, application whitelisting, and DLP.

Companies are increasing their use of cloud and mobile technologies. The research explored the technologies used by the Fortune 500 financial services companies to secure these platforms, and their view of the relative security of these platforms. Utilizing pattern matching, the study noted a consistent theme the interview participants mentioned in the interviews, i.e., mobile and cloud platforms were not experiencing security incidents and breaches. Interview participants regularly utilized MDM and containerization to reduce the threat of security breaches on mobile devices. The participants interviewed also had strong oversight on use of external cloud services, often using IT to monitor usage. Using pattern matching, it was observed that participants mentioned that a cloud service has a more simplistic architecture than their internal legacy systems. Mobile and cloud platforms did not seem to add to security incidents and breaches for the companies interviewed.

All of the interview participants were members of FS-ISAC, and many participated in additional threat-information sharing groups. Using pattern matching, the study

determined that most of the participants could not identify specific information they received from FS-ISAC that stopped a security breach. Participants consistently mentioned the amount of information they received was overwhelming and hard to keep up with. In a few cases, participants highlighted the intelligence and assistance they received from FS-ISAC that pertained to DDOS attacks and how they utilized that information to prevent security incidents. One company identified specific targeted information they received from FS-ISAC that prevented a security breach. A few of the participants were in the early stages of using technology to automatically ingest threat IOCs.

Several questions for future research emerged from this case study: Will opinions of information security leader's change with respect to mobile and cloud services if there are major breaches reported related to these platforms? Would information security leaders from a different industry segment have similar views? As the ingestion of IOCs advances, do security incidents and breaches decline? What are the technical challenges of automating the ingestion of IOCs? If the companies interviewed were challenged with ingesting the threat sharing information, should the government turn their focus to helping companies effectively use the threat information being shared? What is the return on investment of the increased spending on cyber security? Would the chief information officers have a different view of security than the technical leaders of information security? Cyber security provides a wealth of research opportunities.

Based on this case study, IT security does increase awareness of security incidents and breaches. Information security technology also has the ability to decrease security incidents and breaches, and mobile and cloud services do not seem to increase security

incidents and breaches. Companies are overwhelmed with the threat information that they are receiving today but believe belonging to an FS-ISAC will give them access to valuable information that will help with specific threats and understand threat trends.

Major data breaches continue to occur while the U.S. government continues to roll out regulations and guidance with the purpose of improving cyber security. As adversaries increase their capabilities, and hacking tools continue to change and advance, there will continue to be a contest between companies that are trying to secure their enterprise and the hackers who are finding new ways to compromise systems. Sharing security threat intelligence, collaborating on security best practices, and conducting information security research can be used to advance the cyber defenses of public and private industry.

Appendix A

List of Acronyms

APT: Advanced Persistent Threat

ARRA: American Recovery and Reinvestment Act

BYOD: Bring Your Own Device

CERT: Computer Emergency Readiness Team

CFPB: Consumer Financial Protection Bureau

CINS: Critical Infrastructure Notification System

CISO: Chief Information Security Officer

CPU: Central Processing Unit

CSA: Cloud Security Alliance

DDoS: Distributed Denial of Service

DLP: Data Loss Prevention

DMARC: Domain-based Message Authentication, Reporting, and Conformance

DKIM: Domain Keys Identified Mail

DoS: Denial of Service

DTCC: Depository Trust & Clearing Corporation

FBI: Federal Bureau of Investigation

FDIC: Federal Deposit Insurance Corporation

FFIEC: Federal Financial Institution Examination Council

FTC: Federal Trade Commission

FRS: Federal Reserve System

FS-ISAC: Financial Services Information Sharing and Analysis Center

FSOC: Financial Stability Oversight Council

Gbps: Gigabits per second

GLBA: Gramm-Leach-Bliley Act

GSCIS: Graduate School of Computer and Information Sciences

HHS: Health and Human Services

HIPAA: Health Insurance Portability and Accountability Act

IaaS: Infrastructure as a Service

IC3: Internet Crime Complaint Center

IDS: Intrusion Detection System

IOC: Indicators of Compromise

IP: Internet Protocol

IPS: Intrusion Prevention System

IRB: Institution Review Board

ISAC: Information Sharing and Analysis Center

ISACA: Information Systems Audit and Control Association

ISO: International Organization for Standards

IT: Information Technology

MAM: Mobile Application Management

MDM: Mobile Device Management

NCUA: National Credit Union Administration

NIST: National Institute of Standards and Technology

NISTIR: National Institute of Standards and Technology Interagency Report

NCCoE: National Cybersecurity Center of Excellence

OCC: Office of the Comptroller of the Currency

PaaS: Platform as a Service

PCI-DSS: Payment Card Industry-Data Security Standard

PHI: Protected Health Information

PI: Personal Information

PII: Personally Identifiable Information

RQ: Research Question

SaaS: Software as a Service

SEC: Securities and Exchange Commission

SIEM: Security Information and Event Management

SOC: Security Operations Center

SPF: Sender Policy Framework

SSC: Security Standards Council

URL: Uniform Resource Location

US: United States

VM: Virtual Machine

Appendix B

Survey Instrument

RQ 1: What type of information security products result in an increased awareness, providing you the ability to detect security incidents and breaches?

- What information security product capabilities have you implemented in the last three years that increased your awareness to detect security incidents and breaches?
- How has technology allowed you to decrease your company's security exposures?
- How has technology helped you to detect and react to a threat more quickly?
- Do you think you would have found the threat or compromise without the new security technology?
- How has security technology increased your visibility into security incidents and breaches?

RQ 2: What types of security information technology result in a decrease of security incidents and breaches?

- What information security product capabilities have you implemented in the last three years that decreased your security incidents and breaches?
- How has technology allowed you to decrease your company's security exposures?
- How has technology helped you react to a threat more quickly?
- Did the technology alone provide decreased security incidents and breaches, or identify areas that require your company to make process changes to decrease security incidents and breaches?
- How has security technology decreased your security incidents and breaches?

RQ 3: How have new technologies, for example, cloud and mobile technologies, resulted in an increase or decrease in data security incidents and breaches, and has the technology strengthened or weakened enterprise security?

- What cloud and mobile technologies infrastructure changes have been implemented that have security implications in the past three years?
- How have these infrastructure changes increased or decreased security incidents and breaches?
- How would you compare (more robust vs. weaker) the security of your mobile devices to PCs?
- How has technology been applied to your mobile solutions to decrease the risk of security incidents and breaches?
- How would you compare (more robust vs. weaker) the security of your cloud services to your on-premise IT solutions?
- How has technology been applied to your cloud services to decrease the risk of security incidents and breaches?

RQ 4: To what extent can participation in threat information-sharing groups, or threat intelligence information sharing, increase awareness of security incidents and breaches?

- Do you participate in FS-ISAC or another security threat-sharing forum?
- How has the information from threat-sharing forums decreased security incidents and breaches?
- How has the information from threat-sharing forums increased your awareness of security incidents and breaches?
- How has your company been able to stop attacks in progress with the information that you have gained from threat-sharing forums?

Appendix C

Interview Responses

Interview Question 1A: What information security product capabilities have you implemented in the last three years that increased your awareness to detect security incidents and breaches?

A1

- We have installed threat analytic technology to gain more visibility into attacks

A2

- Solutions to search for malicious content for web & email.
- Security incident event management (SIEM) analyzing events across Windows OS, IPS, FW 24x7.
- Forensic endpoint detecting malicious code.
- Next-generation firewalls inside the network to interrogate internal network traffic.
- Technology to monitor active directory to analyze access rights.

A3

- DDOS services (to identify if we are being targeted).
- Advanced malware detection.
- Data leakage prevention.
- Detecting large file transfer out of the network.
- SIEM.
- Vendor doing advanced scanning of network (use two different vendors, swapping back and forth to get different perspectives).

A4

- Security operations center (SOC).
- Security incident event management/log analysis.
- DDOS detection and prevention.
- Decrypting network traffic to interrogate.
- Vulnerability scanning.
- Change audit and threat detection.
- Scanning traffic leaving enterprise.
- Threat detection for endpoint.
- Internet content filtering.

A5

- Network and email threat detection and prevention.
- Security log analysis.
- Network monitoring and detection.
- Professional services to assess our network.
- Multiple threat feeds.
- Upgraded IPSs.

A6

- Sandboxing URLs and binaries.
- Managed services to monitor network traffic.
- Services to prevent command and control communication, malware, and phishing.
- Intrusion detection system (IDS).

A7

- Network APT detection and prevention.
- Analyze employee reported SPAM and analyze the infrastructure for similar emails.
- Endpoint technology that opens attachments and websites in a virtual container, preventing the endpoint being infected with malware.
- DLP on network (non-email web traffic).
- Monitor applications for communication to cloud services, and data transfer outside the company.

A8

- Log aggregation.
- Service to review system for Indicators of Compromise.

A9

- SIEM/log management.
- Netflow analysis.
- IDS.
- Advanced email scanning, able to detect malicious payloads.
- Advanced malware behavior detection.
- Endpoint protections (AV/HIPS/behavior based).

Interview Question 1B: How has technology allowed you to decrease your company's security exposure?

A1

- The threat analytic technology has given us greater visibility into attacks. The threats also have increased with a bigger attack surface. The technology has allowed us to keep up vs. decrease the security exposure.

A2

- Yes. We can track by the number of events that we have a decreasing number of incidents (example, fewer workstation and server rebuilds).

A3

- Yes (hard to quantify).
- DLP: We see data leaving the business showing broken business processes, that we can go back and improve the processes.
- Being able to stop command and control traffic.

A4

- The technology has provided us better insights into threats that exist

A5

- We are able to detect and remediate issues that we would have been unaware of.

A6

- Prior to this newer technology we had only signature based detection, and would not have detected several vulnerabilities.

A7

- We are seeing more details about the security of our infrastructure than we were before, and we are able to react more quickly to the information.
- Not sure we are seeing a decrease, as the attacks are increasing. It is more like a treadmill going faster, and we are trying to keep up.

A8

- Technology has allowed us to have better insight into what we didn't know.

A9

- We have been able to measure improved security through penetration testing results.
- We track 20 critical security controls, and are able to show a decrease in security exposures
- We can show a decrease in security incidents

Interview Question 1C: How has technology helped you detect and react to a threat more quickly?

A1

The technology has allowed us to perform quarantining and isolation faster. The technology allows for better correlation of events across more points of detection. The technology is not 100% effective, but it provides a better data scientific approach to security threats.

A2

We are finding security issues in days/hours vs. months/years.

A3

We are picking up threats earlier in the attack.

A4

Our tools can assess the threat quicker, and we are able to react faster. There is a lack of integration to the tools that makes managing all this information difficult.

A5

We have greater insights into our environment. We continue to add new functions and technologies to provide better insights into security threats.

A6

The newer technology allows us to detect and stop attacks earlier in the delivery phase of the attack.

A7

We have more data to detect information about our infrastructure, and to keep up we have needed to increase staff to analyze the data and take actions.

A8

Log correlation and analytics have allowed us to develop rules for anomalies, and detect/respond to threats early in the attack cycle. Utilizing a service that searches for Indicators of Compromise (IOCs) has allowed us to have better optics to understand if hackers are inside our network.

A9

We have dramatically better awareness of issues and can address issues quicker. We have been able to anticipate issues and prioritize actions more effectively.

Interview Question 1D: Do you think you would have found the threat or compromise

without the new security technology?

A1

The technology has allowed us to find some threats or compromises that we would have not found without it. In some cases, we would have found the threat or

compromise with existing technology, but not as fast. We were able to detect the compromise earlier in the kill chain.

A2

Probably not in all cases. We were not able to look or analyze all the security information prior to this security technology being implemented.

A3

Without some of the technology, we would have been oblivious of the attack. Even with the technology, sometimes humans pick up cases that the technology does not alert on.

A4

We would have been blind to many of these issues.

A5

Several of the issues we found, we would not have been aware of without this additional security technology.

A6

No. The newer technology provided insights we did not have prior.

A7

In some cases, our legacy capabilities would have found the security issue but, in some cases, much later in the attack cycle than we are currently finding the issue.

A8

We would have found some, but the security services that provide Indicators of Compromise scanning has found things our installed technology would not have.

A9

Our penetration testing demonstrates that we are able to find and resolve security issues earlier in the attack cycle.

Interview Question 1E: How has security technology increased your visibility into security incidents and breaches?

A1

With the technology, we were able to detect some threats or comprises earlier in the kill chain or, in other cases, detect when our existing technology would not have found the security threat.

A2

We are able to analyze and have greater visibility into our infrastructure, allowing us to react quicker.

A3

DLP has provided insight into broken business processes that we have been able to address. Malware scanning by a vendor has been able to pick up malware missed by our current anti-virus.

A4

The tools have been able to detect malware issues and patching gaps that we were able to address.

A5

The new tools have found issues that our old software would not have identified.

A6

The newer technology allowed us to detect and stop attacks earlier in the kill chain.

A7

We have much better insight into our network traffic for indicators of concern.

A8

We have been able to detect and respond to events in almost real time (minutes-hours vs. days-months).

A9

Better defense in depth. Broader coverage at detecting security issues. We better understand “normal” and can detect when we are not normal. The insights we have gained from the technology has allowed us to make process improvements. One example is, when employees identify SPAM, we are able to analyze quickly if it is malicious, quickly analyze our network, and remediate.

Interview Question 2A: What information security product capabilities have you implemented in the last three years that decreased your security incidents and breaches?

A1

- We have implemented technology that allows us to keep up on the latest patching information.
- We have done better matching exploits to our infrastructure, improving the effectiveness of our patching program.

A2

- Blocking malicious web sites.
- Blocking command and control sites.
- Dissecting SSL traffic to interrogate for malicious traffic.

- Endpoint whitelisting.

A3

- Privileged user account management/isolation.

A4

- Advanced malware detection, including proactive blocking.
- Blocking uncategorized websites.
- DLP (in some cases we block data flow).
- DLP: We are detecting and changing business processes, but limited blocking.

A5

- Aggressive IP blocking.
- DLP.

A6

- Host intrusion protection systems (HIPS).
- Data leakage prevention (DLP).
- eMail protections to analyze and execute opening email attachments or web links in a safe container to assess the presence of malware to prevent malicious email from entering systems.

A7

- We run an educational program to help employees identify phishing emails, which decreases malware infections.
- DLP for web traffic is used in monitoring mode.
- We block malicious and uncategorized websites.
- Aggressive SPAM filtering.

A8

- DLP (email, endpoint, and network/gateway).
- Whitelisting.
- Next-gen firewalls.
- Web filtering.
- Identify anomalous behavior.

A9

- Application vulnerability scanning.
- IP blocking (reputation, web site blocking).

Interview Question 2B: How has technology allowed you to decrease your company's security exposure?

- A1
We have more quickly and effectively patched the infrastructure in the highest risk areas.
- A2
Reduced malware on endpoints/servers. Reduced the threat of an adversary moving laterally.
- A3
Decreased malware infections.
- A4
The technology has been able to point out areas that need focus, but we are in the early stages to gain all we can from the technology.
- A5
IP blocking has allowed us to prevent security issues by preventing malware and reducing data loss vectors.
- A6
We are stopping malicious email at the gateway.
- A7
We have been able to decrease phishing attacks. We have been able to decrease malware infections that would have happened when employees visited compromised/malicious websites.
- A8
We have been able to detect and respond to user error. We have visibility into events. We have been able to identify flawed processes. We are able to block malicious sites.
- A9
Less security defects in code. Fewer malware infections.

Interview Question 2C: How has technology helped you react to a threat more quickly?

- A1
We target patching the key infrastructure better.
- A2
Fewer alerts from SIEM to alert staff of issues.

- A3
Technology was often just one part of a blended solution of people/process/technology.
- A4
Monitoring DLP traffic has allowed us to understand processes that need to be improved.
- A5
DLP has allowed us to understand broken business processes and provided us the data to work with the business to remediate.
- A6
We are preventing the attacks.
- A7
Using the technology, we are able to analyze who received a malicious email and remediate the threat across the infrastructure.
- A8
We are able to detect issues and prevent malware entering our infrastructure.
- A9
If there are issues from website traffic, we are able to use our information security tools to analyze and address faster.

Interview Question 2D: Did the technology alone provide decreased security incidents and breaches, or identify areas that require your company to make process changes to decrease security incidents and breaches?

- A1
We have practiced security incident tabletops to improve our process readiness of a security incident or breach.
- A2
Alerts to the SIEM allowed the staff to analyze issues and make process changes.
- A3
DLP provided insights to improve the security of business processes. Detecting command and control traffic, and blocking traffic cut off security incidents.

A4

With the data we received from DLP, we were able to engage application owners and development/operations to improve the processes. We were able to influence the software development life cycle (SDLC).

A5

IP blocking decreased security incidents. DLP provided insights to change business process, leading to improved data security.

A6

We have utilized the technology to decrease attacks, and have had limited focus on process changes.

A7

The technology allowed us to react faster to threats. Having employees report phishing emails to a security mailbox has allowed us to clean up the environment and prevent threats from turning into incidents

A8

We have identified flawed processes with our technology that we have been able to improve.

A9

Having real data about security defects in internally developed code has allowed us to gain better partnership with developers to build secure code.

Interview Question 2E: How has security technology decreased your security

incidents and breaches?

A1

Effective patching has decreased security incidents and breaches by decreasing the vectors an attacker can penetrate in our systems.

A2

Can see with metrics that issues and incidents have decreased. We have better visibility to understand the effects of an incident and react or learn from the issue.

A3

Stop attacks in progress. Improve the security of business processes.

A4

Security technology has given us better insights into processes we can improve to reduce security incidents.

A5
The new security technology we have installed has allowed us to prevent malware infections and reduce the chance of unintended data loss.

A6
We have less malware on endpoints.

A7
When we find a threat, we are able to assess and remediate prior to the threat becoming an incident. We are reducing the number of malware infections entering our system.

A8
We have been able to create semi-automatic blocking of malicious email, reducing malware infections.

A9
We have more secure code being developed. We have fewer malware infections, as we are able to prevent through IP blocking

Interview Question 3A: What cloud and mobile technology infrastructure changes have been implemented in the past three years that have security implications?

A1
Increased third-party hosting and cloud hosting has occurred, for example, cloud office suite.

A2
Increased mobile endpoints. Cloud usage to reduce cost and increase speed (examples: HR, CRM).

A3
We utilize mobile for email/calendar/contacts, but we have few mobile applications. Limited cloud usage, unless it has been approved by information security.

A4
We are using mobile technology more. We utilize Android and iOS. We have lots of mobile applications. We are quickly deploying cloud services but are in the early stages.

A5
Mobile: Employee enablement. Cloud: Aggressive adoption.

A6

Mobile: Mail/calendar/contacts and limited applications on mobile. Cloud: We have a policy of cloud first.

A7

Mobile: We are using more mobile devices to support the business needs. Cloud: We are utilizing more SaaS solutions in the cloud.

A8

For BYOD non-managed devices, we have implemented sandboxing. For cloud, we have installed technology to detect any use of public cloud services so we can manage corporate use of external IT infrastructure.

A9

Mobile: BYOD and company owned; MDM and containerization; isolated network traffic. Cloud: Very limited.

Interview Question 3B: How have these infrastructure changes increased or decreased security incidents and breaches?

A1

We have not seen an increase of security incidents and breaches yet.

A2

Mobile is a lower threat than Windows endpoints. Cloud has benefits and risks for security.

A3

No substantial changes. We lock down the mobile device with mobile device management and container technology. Cloud services go through security assessment before they are utilized.

A4

We invested quite a bit to lock down the mobile devices. The mobile devices extend our attack surface, but we need to support the business with more flexible endpoints.

A5

Slight increase in risk, but our approach has not created significant risk.

A6

We have had no evidence of security incidents on mobile or cloud, but I am aware of the attack vectors and risks of these platforms.

A7

In both cases, I believe our risks have increased because of the additional technology. I have not seen an increase in incidents or breaches for mobile or cloud.

A8

For mobile, we have implemented MDM and containerization. Mobile devices are employee owned. For laptops, the majority are owned company owned. If BYOD, they have a virtual connection to the company.

A9

We have not seen any increase of security incidents.

Interview Question 3C: How would you compare (more robust vs. weaker) the security of your mobile devices to PCs?

A1

We have more control over the mobile device with MDM and containerization technology.
To date, we don't have custom mobile applications.

A2

We use an MDM and have limited application development on mobile devices. No containerization. Ecosystem on mobile is much cleaner and more simple than Windows.

A3

We have seen little Android malware entering our enterprise. More robust.

A4

PCs have a greater number of users. Users of PCs have a greater chance of being social engineered, leading to a security incident. Mobile is more locked down.

A5

PCs have more security technology, providing more robust controls. Mobile has many fewer features and more locked down.

A6

I see the risk of PCs and Mobile devices as the same. Both have access to information within the company network.

A7

For PCs, we allow users to have administrative rights. Our PCs have many more controls, but the threat vector is larger on PCs than mobile devices. There are limited functions enabled on mobile devices. I think the controls are proportional to the risks.

A8

I see both mobile and PCs as having strong security. Corporate devices are locked down. Off-shore and BYOD are set up with virtual connections.

A9

PCs are more secure. We have locked down PCs. We utilize virtualization, encryption, and elimination of admin rights to lock down PCs. On mobile devices, users can install applications, and we have less visibility into network traffic

Interview Question 3D: How has technology been applied to your mobile solutions to decrease the risk of security incidents and breaches?

A1

The data that is stored currently is only mail/calendar/contacts. We have MDM and MCM technology to protect the data on the mobile devices.

A2

MDM provides security functions. Limited functions reduce chance of security issues.

A3

We lock down the mobile device with mobile device management and container technology.

A4

We have installed MDM, containerization, and do application vulnerability scanning for mobile applications.

A5

The MDM and containerization provides a strong platform for managing the security of our mobile device.

A6

We have MDM and containerization.

A7

We have an MDM and no container. We have a mobile security solution that prevents malware and targeted attacks.

A8

With PCs and mobile devices, we have locked them down so you cannot copy data or move data outside container.

A9

MDM allows us to manage the security health of the mobile device. Containerization provides protection from data loss.

Interview Question 3E: How would you compare (more robust vs. weaker) the security of your cloud services to your on-premise IT solutions?

A1

Weaker. There is lack of visibility to security due diligence. We lost control and oversight.

A2

Mixed. It depends on the security of the Cloud Service provider. Cloud services could provide more security because you are not concentrating all your IT capabilities within your in-house infrastructure. If a company uses multiple cloud providers, and one cloud provider is compromised, it would not stop all processing/work.

A3

More robust. Cloud solutions have less complex systems because they don't need to deal with legacy systems. Cloud systems have better encryption. We are dependent on what the cloud provider tells you vs. direct oversight.

A4

If cloud services are implemented correctly, they can provide more robust security. Poor governance can lead to weaker cloud security. Our goal is to enable developers to use secure cloud services.

A5

For the cloud solutions we have approved, the security is stronger. Cloud solutions provide the ability to spin up a secure workload quickly.

A6

I see similar levels of risk between on-premise and cloud solutions, especially if the workload is lift-and-shifted to the cloud. We already outsource our IT to a third party, so moving to the cloud was not a change in risk.

A7

Today, we are only using SaaS solutions. We have corporate governance over use of SaaS solutions and have monitoring of cloud service. Cloud solutions are similar risk to providing company data to a third-party.

A8

For cloud services, we have strong policies and processes, we manage the use of external cloud services, and we encrypt the data. I see cloud (both internally hosted

and externally hosted) as more secure, as it is less complex than the legacy infrastructure.

A9

We have not implemented public cloud solutions.

Interview Question 3F: How has technology been applied to your cloud services to decrease the risk of security incidents and breaches?

A1

The cloud has more threats and incidents. There is limited technology to decrease the risks, but I expect more to come in the future. I have not installed specific security technology to the cloud environment.

A2

Technology has been applied between our company infrastructure and the cloud provider to detect security issues/threats.

A3

Cloud systems are not used unless sanctioned and approved by information security. Cloud systems we are utilizing have strong security systems.

A4

We are in the early stages, and are carefully evaluating cloud services for security.

A5

We define specific cloud solutions that are approved by information security. Information security performs detailed analysis and provides governance when using cloud services. All data are encrypted in the cloud.

A6

Cloud services provide good security capabilities; the key is how the application utilizes the security capabilities offered by cloud services. Commercial cloud services have a better security design, testing, and external security certifications than internally developed infrastructure.

A7

We have security solutions that monitor use of cloud solutions. We have limited visibility of the security of SaaS cloud solutions.

A8

Encryption of data. Monitoring use of public cloud services.

A9

We have not implemented public cloud solutions.

Interview Question 4A: Do you participate in FS-ISAC or another security threat sharing forum?

A1

Yes.

A2

Yes.

A3

Yes.

A4

Yes.

A5

Yes. We participate in about 50 threat feeds.

A6

Yes, we belong to FS-ISAC and InfraGard.

A7

Yes.

A8

Yes. We belong to FS-ISAC and Department of Homeland Security. We pay for vendor threat feeds.

A9

Yes.

Interview Question 4B: How has the information from threat sharing forums decreased security incidents and breaches?

A1

At the highest level, very little. We receive the threat information from multiple other sources.

A2

Limited value. Less actionable intelligence. Too many emails/alerts. Better awareness in general about financial services attacks.

A3

We proactively block malware with the threat intelligence we receive.

A4

There is too much data. There is a need for automation. Today, we manually need to analyze too much data. The threat information requires technical talent to make judgments on the information. The information does provide intelligence to decrease threats, but it takes too much effort to analyze.

A5

The threat intelligence feeds allow us to incorporate security controls based on Indicators of Compromise, but there is too much data. The threat intelligence data are hard to manage. It is difficult to sort out the critical and relevant information.

A6

We find limited value because the amount of information is too much to analyze and consume.

A7

We react to FS-ISAC data constantly, for example, block IP addresses.

A8

We analyze and respond with the data we receive from the threat feeds and our relationships with peer companies.

A9

Absolutely. We use the information (Indicators of Compromise) to detect and prevent security issues. We have gained insights into wire-transfer scams to allow us to prevent them.

Interview Question 4C: How has the information from threat sharing forums

increased your awareness of security incidents and breaches?

A1

Day to day, we receive very little unique information. The information I gain from FS-ISAC at a macro level on threats have been more helpful.

A2

Not much. Too much data. Until automated threat sharing is implemented, it is too hard to consume.

- A3
We improved our DDOS controls after receiving insight from FS-ISAC. My team gains value from the professional exchanges they have with other members in FS-ISAC.
- A4
The information provided by the threat sharing forums have provided us better viability and allowed us to take action to respond to the threat.
- A5
Threat information, for example, the increased DDOS threat, allows us to improve our defenses.
- A6
The information has been too much to be useful.
- A7
The data FS-ISAC provides us gives us greater insight into general attacks happening within the financial sector. We have been able to respond with additional security controls from information shared about the attacks against the banking sector.
- A8
The threat information allows us to keep an eye forward to the next set of threats. We gain from information we share with other companies within the sharing forums. We have added hunting activities to our security operations center.
- A9
We have been able to use information from FS-ISAC to educate the business, reducing incidents.

Interview Question 4D: How has your company been able to stop attacks in progress with the information that you have gained from threat-sharing forums?

- A1
Rarely. We do incorporate Indicators of Compromise, but the information we receive is not specifically useful to the company.
- A2
We are able to react to threat information. Information does not allow us to be proactive. Too many emails. It is hard to find useful data.
- A3
I am not aware of any attack in progress we have stopped with FS-ISAC threat intelligence.

A4

Yes. We were involved in two major sporting events. The threat information shared for those events were very actionable, and we were able to update our security controls daily to respond to the threats.

A5

Yes. After we received intelligence on DDOS attacks from FS-ISAC, we were able to improve our defenses.

A6

The information has not helped us stop attacks. No ability to react to the hundreds/thousands of Indicators of Compromise. What the industry needs is a good intelligence management system, which I don't think the vendors have solved yet.

A7

I have no evidence that any information received from FS-ISAC stopped a specific attack against our company.

Today, humans process the information from FS-ISAC. We are working on early stages to automate the consumption of the threat intelligence.

A8

I am not aware of any specific attacks we have stopped. We are in early stages to use STIX and TAXII to automate the ingestion of the threat indicators. We apply all Indicators of Compromise to our infrastructure.

A9

I am not sure we have stopped a specific attack. We have used the information provided by FS-ISAC to defend against DDOS attacks. We improved our defenses. When there was a raised threat, we added additional controls.

Reference List

- Ablon, L., Libicki, M., & Golay, A. (2014). Markets for cybercrime tools and stolen data. *RAND*. Retrieved from https://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf
- Afroz, S., Islam, A., Santell, J., Chapin, A., & Greenstadt, R. (2013). How privacy flaws affect consumer perception. *2013 Third Workshop on Socio-Technical Aspects in Security and Trust*, 10–17. New Orleans, LA: IEEE.
- AirWatch. (2014). *AirWatch by VMware*. Retrieved from <http://www.air-watch.com/>
- Albanesius, C. (2014, April 22). AOL mail hacked, accounts sending spam. *PC Magazine*. Retrieved from <http://www.pcmag.com/article2/0,2817,2456926,00.asp>
- Alfath, A., Baina, K., Baina, S. (2013). Cloud computing security: Fine-grained analysis and security approaches. *2013 National Security Days (JNS3)*, 1–6. Rabat, Morocco: IEEE.
- Alsubibany, S., Morisset, C., & van Moorsel, A. (2013). Detection of attack strategies. *2013 International Conference on Risks and Security of Internet Systems (CRiSIS)*, 1–8. La Rochelle, France: IEEE.
- Amazon Web Services. (2014). *AWS security center*. Retrieved from http://aws.amazon.com/security/?nc1=f_cc
- Amoroso, E. (2013). From the enterprise perimeter to a mobility-enabled secure cloud. *IEEE Security & Privacy*, 11(1), 23-31.
- Andoh-Baidoo, F., Amoako-Gyanpah, K., & Osei-Bryson, K. (2010). How Internet security breaches harm market value. *IEEE Security & Privacy*, 8(1), 36–42.
- Ballabio, G. (2013). Security and availability techniques for cloud-based applications. *Computer Fraud & Security*, 10, 5–7.
- Banham, R. (2014). Cloud computing data breaches currently few. *Business Insurance*. Retrieved from http://www.businessinsurance.com/article/99999999/NEWS070101/399999805#full_story
- Bau, J., Bursztein, E., Gupta, D., Mitchell, J. (2010). State of the art: Automated black-box application vulnerability testing. *2010 IEEE Symposium on Security and Privacy*, 332–345. Oakland, CA: IEEE.
- Bayer, U., Kirda, E., & Kruegel, C. (2010). Improving the efficiency of dynamic malware analysis. *Proceedings from SAC'10*, 1871–1879. New York, NY: ACM.

- Bejtlich, R., Steven, J., & Peterson, G. (2011). Directions in incident detection and response. *IEEE Security & Privacy*, 9(1), 91–92.
- Beuhring, A., & Salous, K. (2014). Beyond blacklisting: Cyberdefense in the era of advanced persistent threats. *IEEE Security & Privacy*, 12(5), 90–93.
- Bluecoat. (2015). SSL visibility appliance. Retrieved from <https://www.bluecoat.com/products-and-solutions/ssl-visibility-appliance>
- Board of Governors of the Federal Reserve System. (2014). *What is the purpose of the Federal Reserve System?* Retrieved from http://www.federalreserve.gov/faqs/about_12594.htm
- Bradley, T. (2014, March 18). Report: Average of 82,000 new malware threats per day in 2013. *PC World*. Retrieved from <http://www.pcworld.com/article/2109210/report-average-of-82-000-new-malware-threats-per-day-in-2013.html>
- Breaux, T., & Baumer, D., (2011). Legally “reasonable” security requirements: A 10-year FTC retrospective. *IEEE Computers & Security*, 30, 178–193.
- Bromium. (2015). *Products overview*. Retrieved from <http://www.bromium.com/products.html>
- Burnham, J. (2013). Gartner publishes 2013 magic quadrant for SIEM. *IBM*. Retrieved from <http://securityintelligence.com/gartner-publishes-2013-magic-quadrant-for-siem/>
- CA Technologies. (2015). *CA data protection*. Retrieved from <http://www.ca.com/us/securecenter/ca-data-protection/details.aspx>
- Cadregari, C., & Cutaia, A. (2011). Every silver cloud has a dark lining: A primer on cloud computing, regulatory and data security risk. *ISACA Journal*, 3, 12–16.
- Caldwell, T. (2014). The true cost of being hacked. *Computer Fraud & Security*, 6, 8–12.
- Cardenas, A., Manadhata, P., & Rajan, S. (2013). Big data analytics for security. *IEEE Security & Privacy*, 11(6), 74–76.
- Chapman, I., Leblanc, S., & Partington, A. (2011). Taxonomy of cyber attacks and simulation of their effects. *Proceedings of the 2011 Military Modeling Simulation Symposium (MMS)*, 73–80. San Diego, CA: Society of Computer Simulations.
- Chaudhuri, S. (2013, November 18). Banks to take part in New York Cybersecurity test. *Wall Street Journal*. Retrieved from <http://online.wsj.com/news/articles/SB10001424052702303985504579205973735595650>

- Check Point. (2013). *Check Point 2013 security report*. Retrieved from <http://sc1.checkpoint.com/documents/security-report/files/assets/common/downloads/publication.pdf>
- Chickowski, E. (2011). *SIEM gathers steam in 2010*. Retrieved from http://www.informationweek.in/security/11-01-13/siem_gathers_steam_in_2010.aspx
- Chickowski, E. (2013, June 20). *Why are we so slow to detect data breaches?* Retrieved from <http://www.darkreading.com/attacks-breaches/why-are-we-so-slow-to-detect-data-breach/240156987>
- CipherCloud. (2014). *Searchable strong encryption*. Retrieved from <http://www.ciphercloud.com/technologies/encryption/>
- Cisco. (2014a). *Security*. Retrieved from <http://www.cisco.com/c/en/us/products/security/index.html>
- Cisco. (2014b). *Cisco ASA content security and control security services module*. Retrieved from <http://www.cisco.com/c/en/us/products/interfaces-modules/asa-content-security-control-csc-security-services-module/index.html>
- Cisco. (2014c). *Data loss prevention*. Retrieved from <http://www.cisco.com/c/en/us/solutions/enterprise-networks/data-loss-prevention/index.html>
- Cisco. (2014d). *Network-based intrusion prevention case study: How Cisco protects data center assets with network-based intrusion prevention systems*. Retrieved from http://www.cisco.com/web/about/ciscoitwork/security/csirt_network-based_intrusion_prevention_system_web.html
- Columbus, L. (2013, February 19). Gartner predicts infrastructure services will accelerate cloud computing growth. *Forbes*. Retrieved from <http://www.forbes.com/sites/louiscolumbus/2013/02/19/gartner-predicts-infrastructure-services-will-accelerate-cloud-computing-growth/>
- Connell, A., & Waits, T. (2013). The CERT assessment tool: increasing a security incident responder's ability to assess risk. *2013 IEEE International Conference on Technologies for Homeland Security (HST)*, 236–240. Waltham, MA: IEEE.
- Constantin, L. (2013, September 26). Malicious browser extensions pose a serious threat and defenses are lacking. *PC World*. Retrieved from <http://www.pcworld.com/article/2049540/malicious-browser-extensions-pose-a-serious-threat-and-defenses-are-lacking.html>
- Constantin, L. (2014, January 9). Security analysis of mobile banking applications reveals significant weaknesses. *PC World*. Retrieved from

- <http://www.pcworld.com/article/2086320/security-analysis-of-mobile-banking-apps-reveals-significant-weaknesses.html>
- Consumer Financial Protection Bureau. (2015). *About Us*. Retrieved from <http://www.consumerfinance.gov/the-bureau/>
- Crosman, P. (2013). Why banks are finally embracing cloud services. *American Banker*. Retrieved from <http://www.pwc.com/us/en/banking-capital-markets/publications/bank-technology-news-cloud.pdf>
- Cybenko, G., & Landwehr, C. (2012). Security analytics and measurements. *IEEE Security & Privacy*, 10(3), 5–8.
- CyberArk. (2014). *Privileged account security solution*. Retrieved from <http://www.cyberark.com/product-detail/privileged-account-security-solution>
- Dai Zovi, D. (2011). Mobile attacks and defense. *IEEE Security & Privacy*, 9(4), 68–70.
- Data Loss db. (2014). What we do. *Open Security Foundation*. Retrieved from <http://www.datalossdb.org/about>
- Dell. (2014). *SecureWorks Next generation firewall*. Retrieved from http://www.secureworks.com/it_security_services/nextgen-firewall/
- Dispensa, S. (2010, March 31). *Four steps to prevent malware threats*. Retrieved from <http://www.eweek.com/c/a/Security/How-to-Reduce-MalwareInduced-Security-Breaches/1/>
- Dittrich, D., Bailey, M., & Dietrich, S. (2011). Building an active computer security ethics community. *IEEE Security & Privacy*, 9(4), 32–40.
- Dixon, B., & Mishra, S. (2013). Power based malicious code detection techniques for smartphones. *2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communication (TrustCom)*, 493–500. Melbourne, Australia: IEEE.
- Doherty, N., & Fulford, H. (2005). Do information security policies reduce the incident of security breaches: An exploratory analysis. *Information Resources Management Journal*, 18(4), 21–39.
- Duncan, A., Creese, S., & Goldsmith, M. (2012). Insider attacks in cloud computing. *2012 IEEE International Conference on Trust, Security and Privacy in Computing and Communication (TrustCom)*, 857–863. Liverpool, England: IEEE.
- Duncan, A., Creese, S., Goldsmith, M., & Quinton, J. (2013). Cloud computing: Insider attacks on virtual machines during migration. *2013 12th IEEE International*

- Conference on Trust, Security and Privacy in Computing and Communication (TrustCom)*, 493–500. Melbourne, Australia: IEEE.
- Eken, H. (2013). Security threats and solutions in cloud computing. *World Congress on Internet Security*, 139–143. Ankara, Turkey: IEEE.
- Elliott, D. (2011). Deterring strategic cyberattack. *IEEE Security & Privacy*, 9(5), 36–40.
- Ellis, T., & Levy, Y. (2009). Towards a guide for novice researchers on research methodology: Review and proposed methods. *Issues in Informing Science and Information Technology*, 6, 323–337.
- EMC². (2013). *RSA Netwitness Financial Services*. Retrieved from <http://www.emc.com/security/rsa-netwitness/rsa-netwitness-financial-services.htm>
- Eslahi, M., Var Naseri, M., Hashim, H., Tahir, N., & Saad, E. (2014). BYOD: Current statue and security challenges. *2014 IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE)*, 189–192. Penang, Malaysia: IEEE.
- Federal Bureau of Investigation. (2014). *Internet Crime Complaint Center (IC3): About Us*. Retrieved from <http://www.ic3.gov/about/default.aspx>
- Federal Deposit Insurance Corporation. (2014). *Compliance manual*. Retrieved at <http://www.fdic.gov/regulations/compliance/manual/pdf/VIII-1.1.pdf>
- Federal Deposit Insurance Corporation. (2015). *Who is the FDIC?* Retrieved from <https://www.fdic.gov/about/learn/symbol/>
- Federal Financial Institution Examination Council. (2006). *Information security*. Retrieved from <http://ithandbook.ffiec.gov/it-booklets/information-security.aspx>
- Federal Financial Institution Examination Council. (2012a). *Enforcement actions and orders*. Retrieved from <http://www.ffiec.gov/enforcement.htm>
- Federal Financial Institution Examination Council. (2012b). *Managed security service providers*. Retrieved from <http://ithandbook.ffiec.gov/it-booklets/outsourcing-technology-services/appendix-d-managed-security-service-providers.aspx>
- Federal Financial Institution Examination Council. (2013). *FFIEC forms cybersecurity and critical infrastructure working group*. Retrieved from <http://www.ffiec.gov/press/pr060613.htm>
- Federal Financial Institution Examination Council. (2015a). *About the FFIEC*. Retrieved from <http://www.ffiec.gov/about.htm>

- Federal Financial Institution Examination Council. (2015b). *Cybersecurity assessment tool*. Retrieved from https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_CEO_Board_Overview_June_2015_PDF1.pdf
- Federal Trade Commission. (2006). *Financial institutions and customer information: Complying with the Safeguard Rule*. Retrieved from <http://business.ftc.gov/documents/bus54-financial-institutions-and-customer-information-complying-safeguards-rule>
- Federal Trade Commission. (2015). *About the FTC*. Retrieved from <https://www.ftc.gov/about-ftc>
- Feiman, J., & Casper, C. (2012, December 20). Magic quadrant for data masking technology. *Gartner*. Retrieved from http://citia.co.uk/content/files/magic-quadrant-for-data-masking-technology_45355302.pdf
- Felt, A., Finifter, M., Chin, E., Hanna, S., & Wagner, D. (2011). A survey of mobile malware in the wild. *SPSM '11 Proceedings of the 1st ACM Workshop on Security and Privacy in smartphones and mobile devices*, 3–14. New York, NY: ACM.
- Fidler, D. (2011). Was Stuxnet an act of war? Decoding a cyberattack. *IEEE Security & Privacy*, 9(4), 56–59.
- Financial Industry Regulatory Authority. (2012). *Regulatory Notice*. Retrieved from <http://www.finra.org/web/groups/industry/@ip/@reg/@notice/documents/notices/p125462.pdf>
- Financial Services Information Sharing and Analysis Center. (2013a). *Homepage*. Retrieved from <https://www.fsisac.com/>
- Financial Services Information Sharing and Analysis Center. (2013b). *Membership benefits*. Retrieved from <https://www.fsisac.com/join>
- Finkle, J. (2013, September 25). Data brokers D&B, LexisNexis, Altegrity report cyber attacks. *FOX Business*. Retrieved from http://www.foxbusiness.com/technology/2013/09/25/data-brokers-db-lexisnexis-altegrity-report-cyber-attacks/?cmpid=prn_aol
- FireEye. (2013a). *FireEye advanced threat report 2H2012*. Retrieved from <http://www.fireeye.com/>
- FireEye. (2013b). *Homepage*. Retrieved from <http://www.fireeye.com/>
- Friedberg, I., & Skopik, F. (2015). Combating advanced persistent threats: From network event correlation to incident detection. *Computers & Security*, 48, 35–57.

- FSOC. (2015). *Annual Report*. Retrieved from <https://www.treasury.gov/initiatives/fsoc/studies-reports/Documents/2015%20FSOC%20Annual%20Report.pdf>
- Future of Privacy Forum. (2014). *De-identification*. Retrieved from <http://www.futureofprivacy.org/de-identification/>
- Gabriel, R., Hoppe, T., Pastwa, A., & Sowa, S. (2009). Analyzing malware log data to support security information and event management: Some research results. *Proceedings of the First International Conference on Advances in Databases, Knowledge, and Data Application*, 108–113. Gosier, Guadeloupe: IEEE.
- Gartner. (2014, January 7). *Gartner says worldwide traditional PC, tablet, ultramobile and mobile phone shipments on pace to grow 7.6 percent in 2014*. Retrieved from <http://www.gartner.com/newsroom/id/2645115>
- Gartner. (2015, September 22). Market guide for user and entity behavior analytics. Retrieved from <https://www.gartner.com/doc/reprints?id=1-2NK6M1R&ct=150922&st=sb>
- Ginovsky, J. (2013). A bank risk manager's view of the cloud. *ABA Journal*. Retrieved from <http://www.ababj.com/management-topics/duties/item/3728-a-bank-risk-manager-s-view-of-the-cloud>
- Goel, S., & Shawky, H. (2009). Estimating the market impact of security breach announcements on firm values. *Information & Management*, 46(7), 404–410.
- Gonsalves, A. (2013, March 1). Prices fall, services rise in malware-as-a-service market. *CSO*. Retrieved from <http://www.csoonline.com/article/729655/prices-fall-services-rise-in-malware-as-a-service-market>
- Good. (2014). *Mobile device management*. Retrieved from <http://www1.good.com/secure-mobility-solution/mobile-device-management.html>
- Grobauer, B., Walloschek, T., & Stocker, E. (2011). Understanding cloud computing vulnerabilities. *IEEE Security & Privacy*, 9(2), 50–57.
- Habib, S., Varadharajan, V., & Muhlhauser, M. (2013). A trust-aware framework for evaluating security controls of service providers in cloud marketplaces. *2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communication (TrustCom)*, 459–468. Melbourne, Australia: IEEE.
- Heikkila, F. (2009). *An analysis of the impact of information security policies on computer security breach incidents in law firms* (Doctoral dissertation). Available from ProQuest Dissertations and Theses database. (UMI No. 3380050)

- Hernandez, P. (2014, December 9). *Microsoft unveils Intune mobile app management container technology*. Retrieved from <http://www.eweek.com/mobile/microsoft-unveils-intune-mobile-app-management-container-tech.html>
- Herzberg, A., & Margulies, R. (2012). Training Jonny to authenticate (safely). *IEEE Security & Privacy*, 10(1), 37–45.
- Holloway, M., & Fensholt, E. (2009). HITECH: HIPAA gets a facelift. *Benefits Law Journal*, 22(3), 85–89.
- Homeland Security (2016). *A glossary of common cybersecurity terminology*. Retrieved from https://niccs.us-cert.gov/glossary#letter_s
- IBM. (2013). *IBM X-Force 2012 trend and risk report*. Retrieved from <http://www-03.ibm.com/security/xforce/downloads.html>
- IBM. (2014a). *IBM Security AppScan*. Retrieved from <http://www-03.ibm.com/software/products/en/appscan/>
- IBM. (2014b). *Managed security services*. Retrieved from <http://www-935.ibm.com/services/us/en/it-services/managed-security-services.html>
- Ibrahim, A., Hamlyn-Harris, J., Grundy, J., & Almorsy, M. (2011). CloudSec: A security monitoring appliance for virtual machines in the IaaS model. *Proceedings of the Network and Systems Security (NSS) 2011 5th International Conference*, 113–120. Milan, Italy: IEEE.
- Idrissi, H., Kartit, A., & Marraki, M. (2013). A taxonomy and survey of cloud computing. *2013 National Security Days (JNS3)*, 1–5. Rabat, Morocco: IEEE.
- Imperva. (2012). *Hackers intelligence initiative* (Monthly trend report #14). Retrieved from http://www.imperva.com/docs/HII_Assessing_the_Effectiveness_of_Antivirus_Solutions.pdf
- Imperva. (2015). *File activity monitor*. Retrieved from <http://www.imperva.com/Products/FileActivityMonitor>
- Information Systems Audit and Control Association. (2012). COBIT5 for information security, preview version. *ISACA*. Retrieved from <https://www.isaca.org/COBIT/Documents/COBIT-5-for-Information-Security-Introduction.pdf>
- InformationWeek. (2012, April 9). 9 most costly financial services data breaches. *InformationWeek*. Retrieved from <http://www.informationweek.com/attacks/9-most-costly-financial-services-data-breaches/d/d-id/1103782?>

- InfraGard. (2016, March 12). *InfraGard: Home*. Retrieved from <https://www.infragard.org>
- International Organization for Standards. (2013). *Introduction to ISO 27002*. Retrieved from <http://www.27000.org/iso-27002.htm>
- Javelin. (2013). *More than 12 million identity fraud victims in 2012 according to latest Javelin Strategy & Research Report*. Retrieved from <https://www.javelinstrategy.com/news/1387/92/1>
- Jeffers, D. (2013, December 20). Cryptolocker grossed up to \$30 million in ransom. *PC World*. Retrieved from <http://www.pcworld.com/article/2082204/crime-pays-very-well-cryptolocker-grosses-up-to-30-million-in-ransom.html>
- Jenkins, C. (2013). The three pillars of a secure hybrid cloud. *Computer Fraud & Security*, 6, 13–15.
- Jin, S., Seol, J., Huh, J., & Maeng, S. (2015). Hardware-assisted secure resources accounting under a vulnerable hypervisor. *Proceedings of the 11th ACM SIGPLAN/SIGOPS International Conference on Virtual Execution Environments*, 201–213. Istanbul, Turkey: ACM.
- Johnson, M., & Pfleeger, S. (2011). Addressing information risk in turbulent times. *IEEE Security & Privacy*, 9(1), 49–57.
- Kancherla, K., & Mukkamala, S. (2013). Image visualization based malware detection. *IEEE symposium on Computational Intelligence in Cyber Space (CICS)*, 40–44. Singapore: IEEE.
- Kassner, M. (2013, December 30). Neverquest banking malware more dangerous than Zeus Trojan. *TechRepublic*. Retrieved from <http://www.techrepublic.com/blog/it-security/neverquest-banking-malware-more-dangerous-than-zeus-trojan/>
- Khalil, I., Kreishah, A., Bouktif, A., & Ahmed, A. (2013). Security concerns in cloud computing. *2013 Tenth International Conference on New Generations (ITNG)*, 411–416. Las Vegas, NV: IEEE.
- Kirk, J. (2012, October 11). Conficker worm still being tracked, but evidence collection slows. *Computer World*. Retrieved from http://www.computerworld.com/s/article/9232277/Conficker_worm_still_being_tracked_but_evidence_collection_slows
- Kitten, T. (2013, January 13). *FS-ISAC on DDoS, account takeover*. Retrieved from <http://www.bankinfosecurity.com/interviews/bill-nelson-i-1758>

- Koch, R., Holzapfel, D., & Rodosek, G. (2011). Data control in social networks. *Proceedings of the 2011 5th International Conference on Network and Systems Security (NSS)*, 274–279. Milan, Italy: IEEE.
- Kothari, P. (2013, January 13). *Cloud computing: How can companies reduce the security risk?* Retrieved from <http://cloudcomputing.sys-con.com/node/2747305>
- Krebs, B. (2013, September 25). Data broker giants hacked by ID theft service. *Krebs on Security*. Retrieved from <http://krebsonsecurity.com/2013/09/data-broker-giants-hacked-by-id-theft-service/>
- Krebs, B. (2014, December 19). FBI: North Korea to blame for Sony hack. *Krebs on Security*. Retrieved from <http://krebsonsecurity.com/2014/12/fbi-north-korea-to-blame-for-sony-hack/>
- Krebs, B. (2015, March 11). Apple pay: Bridging online and big box fraud. *Krebs on Security*. Retrieved from <http://krebsonsecurity.com/2015/03/apple-pay-bridging-online-and-big-box-fraud/>
- Leavitt, N. (2013). Today's mobile security requires a new approach. *IEEE Computer*, 46(11), 16–19.
- Lee, R. (2015). Rethinking computers for cybersecurity. *Computer*, 48(4), 16–25.
- Lemos, R. (2013, December 2). *Threat-intel sharing services emerge, but challenges remain*. Retrieved from <http://www.darkreading.com/threat-intelligence/threat-intel-sharing-services-emerge-but/240161881>
- Leonhard, W. (2013, December 4). Botched Outlook 2013 patches KB 2837618 and KB 2837643 break out of the office reply, free/busy, and more. *InfoWorld*. Retrieved from <http://www.infoworld.com/t/microsoft-windows/botched-outlook-2013-patches-kb-2837618-and-kb-2837643-break-out-of-office-reply-freebusy-and-more-232055>
- Lesk, M. (2012). The clouds roll by. *IEEE Security & Privacy*, 10(3), 84–87.
- Lewis, N. (2012). Access rights—Protect access to your data or lose it: Serious misconceptions about information security. *Computer Fraud & Security*, 11, 8–10.
- Lewis, M. (2013). Characterizing risk. *Proceedings of the Eighth Annual Cyber Security and Information Intelligence (CSIIRW)*, 51. Oak Ridge, TN: IEEE.
- Li, Q., & Clark, G. (2013). Mobile security: A look ahead. *IEEE Security & Privacy*, 11(1), 78–81.

- Longfei, W., Xiaojiang, D., & Xinwen, F. (2014). Security threats to mobile multimedia applications: Camera-based attacks on mobile phones. *IEEE Communications*, 52(3), 80–87.
- Lookout. (2014). *Lookout*. Retrieved from <https://www.lookout.com/>
- Lozito, K. (2011). Mitigating risk: Analysis of security information and event management. *International Journal of Business Intelligence Research*, 2(2), 67–75.
- Mandiant. (2013). *No clearance required: Using commercial threat intelligence in the Federal space*. Retrieved from <https://www.mandiant.com/blog/clearance-required-commercial-threat-intelligence-federal-space/>
- McAfee. (2012). *McAfee threats report: Third quarter 2012*. Retrieved from <http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q3-2012.pdf>
- McAfee. (2013a). *Secure computing solutions: Regulatory compliance*. Retrieved from <http://www.securecomputing.com/compliance/>
- McAfee. (2013b). *SPF, DKIM, and DMARC demystified*. Retrieved from <http://www.mcafee.com/us/resources/solution-briefs/sb-spf-dkim-dmarc-demystified.pdf>
- McAfee. (2014a). *McAfee complete endpoint protection—enterprise*. Retrieved from <http://www.mcafee.com/us/products/complete-endpoint-protection-enterprise.aspx>
- McAfee. (2014b). *McAfee total protection for data loss prevention*. Retrieved from <http://www.mcafee.com/us/products/total-protection-for-data-loss-prevention.aspx>
- McAfee. (2014c). *Cloud Secure*. Retrieved from <http://www.mcafee.com/us/services/cloudsecure.aspx>
- McAfee. (2015a). *McAfee labs threat report*. Retrieved from <http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q4-2014.pdf>
- McAfee. (2015b). *McAfee labs threat report*. Retrieved from <http://www.mcafee.com/us/resources/reports/rp-quarterly-threats-aug-2015.pdf>
- McAfee Labs. (2015). McAfee Labs Threat Report August 2015. Retrieved from <http://www.mcafee.com/us/resources/reports/rp-quarterly-threats-aug-2015.pdf>
- Mearian, L. (2013, July 12). Mobile malware, mainly aimed at Android devices, jumps 614% in a year. *ComputerWorld*. Retrieved from http://www.computerworld.com/s/article/9240772/Mobile_malware_mainly_aimed_at_Android_devices_jumps_614_in_a_year

- Mello, J. (2013, June 7). *Negligence and glitches create 64% of data breaches*. Retrieved from <http://www.csoonline.com/article/734617/negligence-and-glitches-create-64-of-data-breaches>
- Messmer, E. (2013, May 30). Gartner security report: McAfee up, Trend Micro down. *NetworkWorld*. Retrieved from <http://www.networkworld.com/news/2013/053013-gartner-security-survey-270297.html?page=1>
- Messmer, E. (2014, April 4). New Federal rule requires banks to fight DDoS attacks. *NetworkWorld*. Retrieved at <http://www.networkworld.com/news/2014/040414-banks-ddos-280425.html?page=1>
- Microsoft. (2014a). *What is a botnet?* Retrieved from <http://www.microsoft.com/security/resources/botnet-what-is.aspx>
- Microsoft. (2014b). *What is ransomware?* Retrieved from <http://www.microsoft.com/security/portal/mmpc/shared/ransomware.aspx>
- Miller, C. (2011). Mobile attacks and defense. *IEEE Security & Privacy*, 9(4), 68–70.
- Mintz Levin. (2015, January 1). *State data security breach notification laws*. Retrieved from http://www.mintz.com/newsletter/2007/PrivSec-DataBreachLaws-02-07/state_data_breach_matrix.pdf
- Miyamoto, D. (2013). Toward automated reduction of human errors based on cognitive analysis. *Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS)*, 820–825. Taichung, Taiwan: IEEE.
- Moriarty, K. (2011). Incident coordination. *IEEE Security & Privacy*, 9(6), 71–75.
- Moriarty, K. (2013, September 16). Threat-intelligence sharing is dead, and here is how we resuscitate it. *SC Magazine*. Retrieved from <http://www.scmagazine.com/threat-intelligence-sharing-is-dead-and-heres-how-to-resuscitate-it/article/311855/>
- Mustaca, S. (2014). Are your IT professionals prepared for the challenges to come? *Computer Fraud & Security*, 3, 18–20.
- Nair, S., Drew, D., & Verderber, V. (2009). Understanding how to protect web-facing applications: Under the covers of requirement 6.6 of PCI. *ISACA Journal Archives*, 4.
- Nakashima, E., & Douglas, D. (2013, March 1). More companies reporting cybersecurity incidents. *The Washington Post*. Retrieved from http://articles.washingtonpost.com/2013-03-01/world/37371617_1_private-sector-network-security-fifth-third-bank

- National Conference of State Legislators. (2013). *State security breach notification laws*. Retrieved from <http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx>
- National Council of ISACs. (2013). *Homepage*. Retrieved from <https://www.isaccouncil.org>
- National Credit Union Administration. (2015). *About NCUA*. Retrieved from <http://www.ncua.gov/about/Pages/default.aspx>
- National Institute of Standards and Technology Internal Report 8053 (2015). *De-identification of personal information*. Retrieved from <http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8053.pdf>
- National Institute of Standards and Technology. (2010). *Guide to protecting confidentiality of personally identifiable information (PII)* (Special Publication 800-122). Retrieved from <http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf>
- National Institute of Standards and Technology. (2011). *Guide to security for full virtualization technologies* (Special Publication 800-125). Retrieved from <http://csrc.nist.gov/publications/nistpubs/800-125/SP800-125-final.pdf>
- National Institute of Standards and Technology. (2012a). *Computer security incident handling guide* (Special Publication 800-61, Revision 2). Retrieved from <http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf>
- National Institute of Standards and Technology 800-146. (2012). *Cloud computing synopsis and recommendations*. Retrieved from <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-146.pdf>
- National Institute of Standards and Technology. (2012b). *Guide to intrusion detection and prevention systems (IDPS)* (Special Publication 800-94, Revision 1 (Draft)). Retrieved from http://csrc.nist.gov/publications/drafts/800-94-rev1/draft_sp800-94-rev1.pdf
- National Institute of Standards and Technology. (2013a). *News*. Retrieved from <http://www.nist.gov/index.html>
- National Institute of Standards and Technology. (2013b). *Guide to enterprise patch management technologies* (Special Publication 800-40 Revision 3). Retrieved from <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf>
- National Institute of Standards and Technology. (2013c). *Guide to malware incident prevention and handling for desktops and laptops* (Special Publication 800-83,

- Revision 1). Retrieved from <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf>
- National Institute of Standards and Technology. (2013d). *Guidelines for managing the security of mobile devices in the enterprise* (Special Publication 800-124, Revision 1). Retrieved from <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf>
- National Institute of Standards and Technology. (2013e). *Glossary of key information security terms* (NISTIR 7298, Revision 2). Retrieved from <http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf>
- National Institute of Standards and Technology. (2013f). *NIST announces plan to sponsor first cybersecurity FFRDC*. Retrieved from <http://www.nist.gov/itl/nccoe-042213.cfm>
- National Institute of Standards and Technology. (2014a). *NIST releases cybersecurity framework version 1.0*. Retrieved from <http://www.nist.gov/itl/csd/launch-cybersecurity-framework-021214.cfm>
- National Institute of Standards and Technology. (2014b). *Framework for improving critical infrastructure cybersecurity version 1.0*. Retrieved from <http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf>
- NetIQ. (2015). *Privileged user management*. Retrieved from <https://www.netiq.com/products/privileged-user-manager/>
- New York State. (2013). *Governor Cuomo launches inquiry into cyber threats at largest insurance companies*. Retrieved from <http://www.governor.ny.gov/press/05282013-cuomo-launches-inquiry-cyber-threats-insurance-companies>
- Nguyen, J. (2011). Internet privacy class actions: How to manage risk from increasing attacks against online and social media. *The Computer & Internet Lawyer*, 28(9), 8–11.
- Nonaka, M. (2012, October 29). FTC finalizes settlements with companies for exposing sensitive consumer information through installation of peer-to-peer file sharing software. *InsidePrivacy*. Retrieved from <http://www.insideprivacy.com/united-states/ftc-finalizes-settlements-with-companies-for-exposing-sensitive-consumer-information-through-install/>
- Norton. (2014). *Cybercrime Index*. Norton. Retrieved from <http://securityresponse.symantec.com/en/uk/norton/cybercrime/>

- Office of the Comptroller of the Currency. (2011). *Privacy of consumer information*. Retrieved from <http://www.occ.gov/publications/publications-by-type/comptrollers-handbook/pcfi.pdf>
- Office of the Comptroller of the Currency. (2015). *About the OOC*. Retrieved from <http://www.occ.gov/about/what-we-do/mission/index-about.html>
- Office of the Comptroller of the Currency. (n.d.). *Publications*. Retrieved from <http://www.occ.gov/publications/index-publications.html>
- Ohlhorst, F. (2013, March 1). *Next-generation firewalls 101*. Retrieved from <http://www.networkcomputing.com/security/next-generation-firewalls-101/240149730>
- Olsik, J. (2013, September 25). Networking nuggets and security snippets. *NetworkWorld*. Retrieved from <http://www.networkworld.com/community/blog/big-data-security-analytics-faq>
- O'Neill, M. (2014). The Internet of things: Do more devices mean more risks? *Computer Fraud & Security*, 1, 16–17.
- Oracle. (2015). *Oracle data masking and subsetting*. Retrieved from <http://www.oracle.com/us/products/database/data-masking/overview/index.html>
- Pagliery, J. (2014, May 6). iPhone bug leaves email vulnerable. *CNN*. Retrieved from <http://money.cnn.com/2014/05/06/technology/security/apple-email-bug/>
- Palo Alto. (2015). *PA-7050 Overview*. Retrieved from <https://www.paloaltonetworks.com/products/platforms/firewalls/pa-7050/overview.html>
- Parks, R., & Duggan, D., (2011). Principles of cyberwarfare. *IEEE Security & Privacy*, 9(5), 30–35.
- PCI Security Standards Council. (2006). *About Us*. Retrieved from https://www.pcisecuritystandards.org/organization_info/index.php
- Peng, S., Wang, G., & Yu, S. (2013). Modeling malware propagation in smartphone social networks. *Journal of Computer and Systems Science*, 79(5), 586–595.
- Ponemon Institute. (2014). *Cost of data breach survey*. Retrieved from <http://public.dhe.ibm.com/common/ssi/ecm/se/en/sel03027usen/SEL03027USEN.PDF>
- Ponemon Institute. (2015). *Cost of a data breach survey*. Retrieved from <http://public.dhe.ibm.com/common/ssi/ecm/se/en/sew03053wwen/SEW03053WWE N.PDF?>

- Privacy Rights Clearinghouse. (2015). *Chronology of data breaches 2005-present*. Retrieved from <http://www.privacyrights.org/data-breach>
- PwC. (2013). *The top ten technology trends for business*. Retrieved from <https://www.pwcaccelerator.com/pwccaccelerator/docs/digital-iq-trends.pdf>
- PwC. (2015). *The global state of information security survey 2016*. Retrieved from <http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html>
- Radcliff, D. (2012). *The SANS 8th annual log and event management survey results revealed!* Retrieved from <http://www.sans.org/press/event-management-survey-results.php>
- Rahmani, A., Amine, A., & Hamou, M. (2015). De-identification of textual data using immune system for privacy preserving in big data. *2015 IEEE International Conference on Computational Intelligence & Communication Technology*, 112–116. Ghaziabad, India: IEEE.
- Reeves, J., & Stark, J. (2011). *How boards can prepare for new SEC cybertheft disclosure requirements*. Retrieved from https://www.boardmember.com/Article_Details.aspx?id=6937
- Ring, T. (2014). Threat intelligence: Why people don't share. *Computer Fraud & Security*, 3, 5–9.
- Roman, J. (2013). *NIST analyzes cybersecurity framework comments*. Retrieved from <http://www.bankinfosecurity.com/developing-security-best-practices-a-5775/op-1>
- Romeo, P., & Parrino, R. (2012). SEC issues guidance on disclosure of cybersecurity risk and cyber incidents. *The Computer & Internet Lawyer*, 29(1), 23–25.
- Romer, H. (2014). Best practices for BYOD security. *Computer Fraud & Security*, 1, 13–15.
- Roos, G. (2013, July 2). *Companies lack real-time breach-detection capabilities: Survey*. Retrieved from <http://www.eweek.com/security/companies-lack-real-time-breach-detection-capabilities-survey/>
- Ryan, M. (2011). Cloud computing privacy concerns on our doorstep. *Communications of the ACM*, 54(1), 36–38.
- Sadiku, M., Musa, S., & Momoh, O. (2014). Cloud computing: Opportunities and challenges. *IEEE Potentials*, 33(1), 34–36.

- SafeNet. (2015). *Data at rest encryption*. Retrieved from <http://www.safenet-inc.com/data-encryption/data-at-rest-encryption/>
- Savitz, E. (2011, November 3). *5 questions boards should ask about data privacy risks*. Retrieved from <http://www.forbes.com/sites/ciocentral/2011/11/03/5-questions-boards-should-ask-about-data-privacy-risks/>
- Schwartz, M. (2013, April 4). *Banks hit downtime milestone in DDoS attacks*. Retrieved from <http://www.informationweek.com/security/attacks/banks-hit-downtime-milestone-in-ddos-att/240152267>
- Seltzer, L. (2012, July 25). *NFC phone hacking and other mobile attacks*. Retrieved from <http://www.informationweek.com/personal-tech/wireless/nfc-phone-hacking-and-other-mobile-attac/240004386>
- Seltzer, L. (2014, August 7). *Free service gives decryption keys to Cryptolocker victims*. ZDNet. Retrieved from <http://www.zdnet.com/article/free-service-gives-decryption-keys-to-cryptolocker-victims/>
- Singer, N. (2013, March 30). *An American quilt of privacy laws, incomplete*. Retrieved from http://www.nytimes.com/2013/03/31/technology/in-privacy-laws-an-incomplete-american-quilt.html?pagewanted=all&_r=0
- Smith, G. (2013, January 23). “Gozi” virus creators charged by FBI with stealing millions from online banking customers. *Huffington Post*. Retrieved from http://www.huffingtonpost.com/2013/01/23/gozi-virus-fbi_n_2535282.html
- Snyder, J. (2012, May 7). *Next-gen firewalls: Off to a good start*. Retrieved from <http://www.networkworld.com/reviews/2012/050712-firewall-test-258613.html?page=1>
- Soltra. (2015). *About Soltra*. Retrieved from <https://soltra.com/>
- Spikes. (2015). *AirGap browser isolation system*. Retrieved from <https://spikes.com/index.html>
- Steiner, P. (2014). Going beyond mobile device management. *Computer Fraud & Security*, 4, 19–20.
- Stevens, D. (2011). Malicious pdf documents explained. *IEEE Security & Privacy*, 9(1), 80–82.
- Stevens, G. (2012). *Federal information security and data breach notification laws* (CRS Publication No. R42475). Retrieved from <http://www.fas.org/sgp/crs/misc/R42475.pdf>

- Strohm, C. (2013, May 8). *Advanced cyber attack tools seen available to hackers*. Retrieved from <http://www.bloomberg.com/news/2013-05-08/advanced-cyber-attack-tools-seen-available-to-hackers.html>
- Suby, M. (2013). The 2013 (ISC)² global information security workforce study. *Frost & Sullivan, and Booz, Allen, & Hamilton*. Retrieved from [https://www.isc2.org/uploadedFiles/\(ISC\)2_Public_Content/2013%20Global%20Information%20Security%20Workforce%20Study%20Feb%202013.pdf](https://www.isc2.org/uploadedFiles/(ISC)2_Public_Content/2013%20Global%20Information%20Security%20Workforce%20Study%20Feb%202013.pdf)
- Symantec. (2010). *Importance of corporate security policy*. Retrieved from <http://www.symantec.com/avcenter/security/Content/security.articles/corp.security.policy.html>
- Tahboub, R., & Saleh, Y. (2014). Data leakage/loss prevention systems (DLP). *2014 World Congress on Computer Applications and Information Systems (WCCAIS)*, 1–6. Hammamet, Tunisia: IEEE.
- Tankard, C. (2014). New rules for combating new threats. *Computer Fraud & Security*, 4, 14–16.
- TechTarget. (2015). *Indicators of compromise (IOC) definition*. Retrieved from <http://searchsecurity.techtarget.com/definition/Indicators-of-Compromise-IOC>
- Track the Money. (2013). *The Recovery Act*. Retrieved from http://www.recovery.gov/About/Pages/The_Act.aspx
- Trend Micro. (2015). *Enterprise mobile device management & security*. Retrieved from <http://www.trendmicro.com/us/enterprise/product-security/mobile-security/device-management/index.html>
- Tripwire. (2015). *Tripwire file integrity monitoring*. Retrieved from <http://www.tripwire.com/it-security-software/scm/file-integrity-monitoring/>
- Trope, R., & Humes, S. (2013). By executive order: Delivery of cyber intelligence imparts cyber responsibility. *IEEE Security & Privacy*, 11(2), 63–67.
- Tse, A. (2014, March 18). Winners of the growing data masking market. *The Street*. Retrieved from <http://www.thestreet.com/story/12532159/1/winners-of-the-growing-data-masking-market.html>
- U.S. Congress. (2015). *S.754—Cybersecurity Information Sharing Act of 2015*. Retrieved from <https://www.congress.gov/bill/114th-congress/senate-bill/754>
- U.S. Cyber Emergency Response Team. (2014). *National cyber awareness system*. Retrieved from <http://www.us-cert.gov/ncas>

- U.S. Department of Health and Human Services. (2013a). *Health information privacy: HITECH act enforcement interim final rule*. Retrieved from <http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitechenforcementiftr.html>
- U.S. Department of Health and Human Services. (2013b). *Health information privacy: Summary of the HIPAA security rule*. Retrieved from <http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html>
- U.S. Government Accountability Office. (2007). *Personal information: Data breaches are frequent, but evidence of resulting identity theft is limited; however, the full extent is unknown*. Retrieved from <http://www.gao.gov/new.items/d07737.pdf>
- U.S. Securities and Exchange Commission. (2011). *CF disclosure guidance: Topic no. 2*. Retrieved from <http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm>
- U.S. Securities and Exchange Commission. (2013). *What we do*. Retrieved from <http://www.sec.gov/about/whatwedo.shtml#VSkVL410yT8>
- U.S. Securities and Exchange Commission. (2015). *Cybersecurity guidance*. Retrieved from <http://www.sec.gov/investment/im-guidance-2015-02.pdf>
- U.S. Senate. (2014). *A "kill chain" analysis of the 2013 Target data breach*. Retrieved from http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=24d3c229-4f2f-405d-b8db-a3a67f183883
- van Kessel, P., & Allan, K. (2013). Under cyber attack, EY's global information security survey 2013. *EY*. Retrieved from [http://www.ey.com/Publication/vwLUAssets/EY_-_2013_Global_Information_Security_Survey/\\$FILE/EY-GISS-Under-cyber-attack.pdf](http://www.ey.com/Publication/vwLUAssets/EY_-_2013_Global_Information_Security_Survey/$FILE/EY-GISS-Under-cyber-attack.pdf)
- Varonis. (2013). *Varonis, DatAdvantage for Windows*. Retrieved from <http://www.varonis.com/products/datadvantage/windows/>
- Verizon. (2013). *2012 data breach investigation report*. Retrieved from <http://www.verizonenterprise.com/DBIR/2013/>
- Verizon. (2015). *2015 data breach investigations report*. Retrieved from <http://www.verizonenterprise.com/DBIR/2015/>
- Vijayan, J. (2014a, March 14). Major companies, like Target, often fail to act on malware alerts. *Computerworld*. Retrieved from http://www.computerworld.com/s/article/9246942/Major_companies_like_Target_ofTEN_fail_to_act_on_malware_alerts

- Vijayan, J. (2014b, February 6). Target breach happened because of a basic network segmentation error. *Computerworld*. Retrieved from http://www.computerworld.com/s/article/9246074/Target_breach_happened_because_of_a_basic_network_segmentation_error
- Vormetric. (2015). *Vormetric tokenization*. Retrieved from <http://www.vormetric.com/products/tokenization>
- Wang, B., Zheng, Y., Wenjing, L., & Hou, Y. (2014). DDoS attack prevention in the era of cloud computing and software-defined networking. *2014 IEEE 22nd International Conference on Network Protocols*, 624–629. Raleigh, NC: IEEE.
- Weis, J., & Alves-Foss, J. (2011). Securing database as a service. *IEEE Security & Privacy*, 9(6), 4–55.
- WhatIs. (2016). *Cryptocurrency*. Retrieved from <http://whatis.techtarget.com/definition/cryptocurrency>
- White House. (2013). *Executive order improving critical infrastructure cybersecurity*. Retrieved from <http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>
- Wiant, T. (2005). Information security policy's impact on reporting security incidents. *Computers & Security*, 24(6), 448–459.
- Willems, E. (2013). Android under attack. *Computer Fraud & Security*, 11, 13–15.
- Wilson, T. (2013, May 9). *Five questions to ask when choosing a threat intelligence service*. Retrieved from <http://www.darkreading.com/threat-intelligence/five-questions-to-ask-when-choosing-a-th/240154527>
- Xu, K., Yao, D., Ma, Q., & Crowell, A. (2011). Detecting infection onset with behavior-Based Policies. *Proceedings of the Network and Systems Security (NSS) 2011 5th International Conference*, 57–64. Milan, Italy: IEEE.
- Yin, R. (2014). *Case study research: Design and methods*. Los Angeles, CA: Sage.
- Yu, S., Gu, G., Barnawi, A., Guo, S., Stojmenovic, I. (2015). Malware propagation in large-scale networks. *IEEE Transactions in Knowledge Data Engineering*, 27(1), 170–179.
- Zhao, T., Zhang, G., & Zhang, L. (2014). An overview of mobile devices security issues and counter measures. *2014 International Conference on Wireless Communications and Sensor Networks*, 439–443. Wuhan, China: IEEE.

- Zheng, M., Sun, M., & Lui, J. (2013). DroidAnalytics: A signature based analytic system to collect, extract, analyze, and associate Android malware. *2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 163–171. Melbourne, Australia: IEEE.
- Zhou, Y. & Jiang, X. (2012). Dissecting android malware: Characterization and evolution. *2012 IEEE Symposium on Security and Privacy*, 95–109. San Francisco, CA: IEEE.