View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by UT Digital Repository

Copyright

by

Robert Dutcher Stiles, Jr.

2018

The Report Committee for Robert Dutcher Stiles, Jr.
Certifies that this is the approved version of the following report:

Information Security Trust and Outcomes:
A Case Study of Compliance in a Complex System

APPROVED BY
SUPERVISING COMMITTEE:

Supervisor:

Hüseyin Tanriverdi

Carolyn Ferguson

Information Security Trust and Outcomes:
A Case Study of Compliance in a Complex System

by

Robert Dutcher Stiles, Jr.

Report

Presented to the Faculty of the Graduate School of

The University of Texas at Austin

in Partial Fulfillment

of the Requirements

for the Degree of

Master of Science in Identity Management and Security

The University of Texas at Austin

May 2018

Abstract

Information Security Trust and Outcomes: A Case Study of Compliance in a Complex System

Robert Dutcher Stiles, Jr., MSIMS

The University of Texas at Austin, 2018

Supervisor: Hüseyin Tanriverdi

As recent high-profile data breaches illustrate, an organization that complies with information security control frameworks can also suffer from successful attacks and the subsequent erosion of trust. Information security frameworks used in the federal, payment, and health care industries use a core catalogue of security controls to standardize practices and facilitate assessment. In theory, an organization implementing these standard controls and practices would maintain sufficient security to protect sensitive data. However, these catalogues of controls require resources to implement and change slowly compared to the evolution of technology and threats. Viewed as a static set of rules in a dynamic complex system, the implementation of catalogues of controls may not create predictable outcomes, or act as reliable indicators of the quality of an organization's security program. I used a case study approach to analyze an organization's security outcomes during a period when control catalogue implementation

transitioned from a best practice to a regulatory mandate I analyzed the organization through the perspective of a complex adaptive system, identifying the complex properties of the organization and its information security team as they endeavored to ensure strict compliance with the control catalogues. I collected data on factors related to the organization's security outcomes, as well as finances, strategy, and governance. Despite significant changes in IT intensity, strategy, and corporate leadership, the security outcomes faltered and recovered, as emergent processes evolved from the dynamic environment. The compliance results, however, were ambiguous. The formal third-party compliance assessment presented outcomes that overstated the impact of isolated controls from the catalogue, while failing to highlight the broader issues related to organizational risk. This prevented the compliance assessment from representing the true state of security of the organization's systems. I conclude that the current method of assessing the quality of an organization's information security program against a control catalogue does not provide sufficient information to establish meaningful trust between organizations. Alternate method that requires a broader perspective of risk may improve the reliability of assessments and provide a more meaningful method to communicate trust.

Table of Contents

List of Tables vii

List of Figures viii

Introduction 1

Literature Review 8

Theoretical Background 13

Methodology 19

Results 39

Discussion 60

Conclusion 70

Bibliography 71

List of Tables

Table 1 YZ Corporation Timeline 28
Table 2 Interviews with YZ employees 30
Table 3 Organization of Results 39
Table 4 Information Security Variables 40
Table 5 Financial Measures in Thousands of Dollars 40
Table 6 Values of Normalized Results 42
Table 7 Penetration Test Details 43
Table 8 FISMA Assessment Results 45
Table 9 Internal Audit Assessments 48
Table 10 Privacy and Security Incidents by Type 50

List of Figures

Figure 1 Graph of Normalized Values 41

Figure 2 Incident Data by Type 2013-2017 50

INTRODUCTION

Equifax is one of the three primary credit reporting agencies in the US, maintaining data on over 800 million individuals, with over 88 million business customers. In July 2017, Equifax's security team became aware that unauthorized individuals had exploited a vulnerability in the Apache Struts software that supported an internet consumer application. Later investigation identified that the exploit of this vulnerability eventually led to the disclosure of the personal financial profiles of over 145 million consumers (Equifax, 2017a). While the attack and investigations were ongoing, Equifax continued to tout their high level of information security compliance on its website. Equifax promoted their consumer and business products with certifications of SOC 2 Type II, ISO 27001:2013, and an Authority to Operate under the FISMA's standards. These certifications required the independent assessment of hundreds of individual security controls and processes defined by the Association of Independent Certified Public Accountants (AICPA), the International Organization for Standardization (ISO), and the National Institute of Standards and Technology (NIST), respectively. The certifications signaled that not only did Equifax believe the data was secure, these institutions came in and proved it. Equifax accompanied the certifications with their statement that "[l]eadership in security is fundamental to our basic purpose – empowering businesses and consumers with information they can trust." As news of the

data breach spread, customer trust in Equifax's security certifications crumbled. In the November 2017 filing with the SEC, Equifax interim CEO stated that Equifax has "an important journey in front of us to regain the trust and confidence of consumers and our business customers" (Equifax, 2017b).

Equifax was in simultaneous compliant and breached states. Despite its adherence to compliance standards Equifax breached the trust of its business partners and 140 million consumers. This paper will examine how organizations, collected together in "trust frameworks," use certifications that assess against control catalogues to signal and communicate trust, and whether compliance with these catalogues and certifications have a reliable and constant impact on security outcomes. Recent research on security breaches using the growing datasets of security failures currently dwarfs the research on compliance and the structure of security regulations. The existing academic and industry control catalogue research focuses on efficient and effective implementation of catalogues of controls, and not whether these catalogues achieve a goal of improving security outcomes. Organizations assume, and do not question, the guaranteed effectiveness of the control catalogues

Research into the fundamental effectiveness of security compliance control catalogue frameworks may be rare for several reasons. Challenges include the difficulty in acquiring the detailed information on compliance implementations, and the relative immaturity of the field of security compliance. The issues of security compliance fundamentals and the structure of the compliance requirements are nonetheless critical in enabling cost-effective business over the internet.

Groups of organizations described as "trust frameworks" develop compliance frameworks, including control catalogues (Leszcz, 2017). Trust frameworks develop a common set of rules to govern a set of business processes between organizations. The value of a common framework is to avoid the need for each organization to conduct due diligence on every other participating organization, while providing common formats for data transfer, rules for processing, and levels of information security.

For information security, the frameworks are often supported by a detailed control catalogue. In this paper, I define control catalogues as lists of computer security practices designed to protect information and systems. The control catalogue developed for compliance with the Federal Information Security Management Act (FISMA) defines a control as "a safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements" (Ross, 2013). The frameworks collect these individual safeguards into a list, grouped together by process or control objective. Control catalogues are part of the security compliance frameworks for federal contractors and agencies (NIST Special Publication 800-53 Appendix F and J), entities involved in payment card processing (PCI-DSS), cloud service providers that wish to store federal data (FEDRAMP), and health care providers and their business associates (HIPAA Security Rule and HITECH). Voluntary compliance frameworks like the ISO 27000 series and the omnibus compliance certification HITRUST include control catalogues in their frameworks as well. A perspective on these frameworks would be to

provide a common set of security best practices for organizations to meet a variety of security needs.

The goal of a common set of best practices may not be met, as each catalogue evolve to meet different data protection requirements. An examination of a control across various control catalogues can demonstrate the variety of approaches to the same protection. Passwords are a common control and addressed by nearly all control catalogues. The ISO 27002:2013 standard's reference control for passwords includes guidance on seven requirements. The requirement for password quality includes five properties, including "easy to remember" and "not vulnerable to dictionary attacks" (International Organization for Standardization, 2013). The Identification and Authentication control (IA-5) for FISMA compliance digs deeper. IA-5 contains 10 requirements for an organization to develop an authenticator. In addition, a moderate implementation includes four control enhancements. Control enhancement IA-5(1) lists five requirements for passwords, including requirements for the organization to define password complexity, to only store and transmit encrypted passwords, and to prohibit password reuse (Ross, 2013). The PCI-DSS v3.2 Requirement 8 specifies the password requirements in greater detail. The 24 parts of Requirement 8 leave less to the organization's discretion. It defines complexity as "at least seven characters" and "contains both numeric and alphabetic characters" (PCI Security Standards Council, 2016). This variety of guidance from organizations demonstrates that there is not a common approach to the simple control of defining a user password.

For most organizations, implementing a single information security framework is not optional. The United States' sectoral approach to privacy and security regulation, combined with individual contract requirements, ensures that an organization that stores or processes data on individuals will implement at least one of these control catalogues. Mapping these controls from one compliance framework to another spawned a small industry, including the HITRUST framework (HITRUST, 2017), which provides certifications across its meta-framework that includes HIPAA, PCI-DSS, and ISO catalogues. Certifications for individuals to map controls from one catalogue to another developed to address the issue of compliance with multiple control catalogues ((ISC)2, n.d.).

The task of sorting through the myriad controls falls on an organization's information security team. These information security teams must then justify the resources to implement and assess these frameworks to help establish business trust, minimize compliance risk, and assist in communicating information security performance to management. Compliance certifications establish trust between business partners, as mentioned in the Equifax case, and are often part of a vendor management program. Certifications like the ISO 2700 series and AICPA's Service Organization Controls (SOC) provide the outside world a glimpse at an organization's interior information security processes and controls. The AICPA identifies three customers for its 2017 SOC for cybersecurity attestation: investors, business partners, and industry regulators: three parties that business must establish trust to succeed (AICPA, 2017). Secondly, the cost and impact of failure to comply with these control frameworks vary significantly by

industry. Frameworks like PCI-DSS for payment cards, and FISMA for federal agencies and contractors require annual certifications by third parties designated or certified by the regulator. The risk of non-compliance is significant, as the federal government can terminate a contract or increase an agency's audit burden, while the PCI can assess fines, or prevent a company from accepting payment cards. Other regulators wait for violations to come to their attention before acting. For example, HIPAA for health information, or the FTC for non-bank financial institutions under the GLBA rely on an institution to self-report, or other public disclosures. Finally, management can use the maintenance of a security framework as a clear and visible measure of information security. Establishing metrics and communicating effectiveness of an information security program continues to challenge corporate information security teams. Reporting activities benchmarked against an externally defined security framework provide a shortcut to demonstrate to management that the information security program is working.

The benefits of trust, compliance risk mitigation, and reporting are designed into most information security frameworks and their control catalogues. However, the primary principle behind all the frameworks is to establish a baseline of information security. The FISMA framework contains a typical statement, that "security controls are the safeguards/countermeasures prescribed for information systems or organizations that are designed to: (i) protect the confidentiality, integrity, and availability of information that is processed, stored, and transmitted by those systems/organizations; and (ii) satisfy a set of defined security requirements" (Ross, 2013). So, the question is, does this method of prescribing control catalogues meet the objective of improved security? What

relationship, if any, exists between an organization's investment in control catalogue compliance and the security of the organization's information assets?

I study this question through a case study of an organization's implementation of the FISMA catalogue of controls. I review data on how the organization measures their success, communicates information security to management, and governs information technology while the organization engages in changes to strategy, leadership, and regulatory burden. I also review measures of security outcomes, including penetration tests and the FISMA assessments. I analyze this data from the perspective of the organization as a complex adaptive system.

The paper begins with a discussion of the current research on information security outcomes and compliance. I introduce the theory of information security as a complex system to frame the research. I define the questions regarding the impact of control catalogues on security outcomes and propose a hypothesis. I introduce the case study, including the background of the organization and the data collection methods. I present the results and demonstrate the relationship between these variables as the organization undergoes changes in strategy, leadership, and regulation. Finally, I discuss the outcomes, and conclude on the hypothesis.

LITERATURE REVIEW

The young field of information security and information security compliance presents several challenges in examining prior research. As a young field, the body of research is not extensive, and a consensus approach to research is not common. The discipline's youth contributes to a lack of a shared lexicon. For example, the literature often uses the words "cybersecurity," "data security," and "information security" to describe the same concept. A variety of disciplines, primarily business and computer science, brings its own set of theories and methods to researching information security.

An early example of research into the dynamics between controls, compliance, and trust addressed the US military's standards for security for computer systems developed by contractors, commonly called "The Orange Book" and later, as it expanded outside the military, "Common Criteria." These standards may not have achieved their goal of a "rich supply of high-assurance systems," but research indicated that they did "move the bar by motivating vendors to include security controls in their products" (Lipner, 2015). Ross Anderson addressed the failings of Common Criteria certification for systems in 2001, identifying the "perverse incentives" and economic pressures between the certifying body and system vendor. These factors, he argues, may lead to certifications that are "irrelevant, erroneous or misleading" (Anderson, 2001).

Heartland Systems suffered a high-profile breach of payment card data in 2008. Robert Carr, Heartland's CEO, discussed the benefits and pitfalls of the PCI standard from his perspective in 2010. Carr acknowledged the utility of PCI controls as establishing a "minimum standard," but identified opportunities for improvement in the

PCI process that assesses compliance. Certified assessors deemed Heartland compliant over a period of years without identifying the flaw in Heartland's system that led to the data breach (Cheney, 2010). In support of discussion by US lawmakers on policy options in the wake of the Target, Sony, JPMorgan, and other data breaches, the Congressional Research Service (CRS) provided research that demonstrated the unsettled nature of establishing effective security controls for payment systems. This research provided four different estimates of the cost of the breach to Target ranging from $4.9 billion to $11 million, pulling from three different researchers and Target itself. The CRS also identified the weakness with the magstripe and signature method of payment card verification, and cited the industry's reluctance to adapt more secure standards based on cost and convenience (Weiss, N.E. and Miller, R.S., 2015). Verizon Business, a PCI certified assessor, publishes an annual report on the state of PCI compliance, based on their assessment activities. This research charts a positive trend in the ability of organizations to maintain compliance with the standards, but the trend started at a low point. In 2011, 11% of organizations were compliant when Verizon conducted the interim assessment. By 2017, the compliant percentage rose to 55% (van Oosten, 2017). The rise of catalogues of controls to improve security outcomes appear to be met by challenges to their effectiveness and the ability to provide accurate assessment.

In 2008, IBM's Klaus Julisch announced security compliance as the next frontier in security research. While that frontier still appears unsettled, Julisch's paper provided a useful definition of security compliance as "the state of conformance with externally imposed functional security requirements and of providing evidence (assurance) thereof"

(Julisch, 2008). His subsequent paper on compliance by design (Julisch, Suter, Woitalla, and Zimmermann, 2011) focused primarily on a method of reliable implementation of control frameworks, rather than determining the effectiveness or adequacy of the framework. Likewise Coffman approached methods for developing a "risk aware" compliance system to remediate computer system vulnerabilities, with a focus on maximizing compliance efficiency with limited resources through risk calculations (Coffman, Agrawal, and Schaffa, 2013). Hayden outlined a method to manage the implementation of multiple control frameworks through a common control framework, since the control frameworks all identify similar security best practices (Hayden, 2009). Solis suggested that the implementation of automated controls for compliance saves money and provides an opportunity for "operational excellence" (Sollis, 2010). Promoters of quantifiable risk assessments for information security view the assessor as just another threat, to be measured and mitigated accordingly. Aligned with this perspective, they see little value in control framework adoption, since the frameworks fail to "describe the nature of the controls, the relationship between controls, or how to measure/estimate the effectiveness of controls within a risk analysis" (Freund and Jones, 2015). Two venerable computer security scientists, Steve Lipner and Butler Lampson, responded to NIST's Commission on Enhancing National Cybersecurity request for input on FISMA guidelines by stating that the "ultimate test of a cybersecurity program is how well it protects systems and information, and current government practices are not passing this test." Lipner and Lampson specifically called out the control catalogues in the FISMA guidance (NIST SP 800-53) and cited the information security failures at the

State Department, Office of Personnel Management, and IRS (Lipner and Lampson, 2016).

Another research approach to the problem of information security compliance examines security failures. Information security researchers examine the newly available data on security failures and data breaches. Sources like Verizon Business' annual Data Breach Report and the Data Breach Clearinghouse provide an ongoing chronicle of security failure. Predictive models for data breaches built on this data provide a risk score for security failures (Liu et al., 2015). The goal of this model is to predict breaches, rather than to identify causal elements that would assist in identifying patterns of failure, including compliance failures, within the organizations examined.

The breach data research dispels some underlying assumptions regarding the trends in security breach impact and frequency (Edwards, Hofmeyr, & Forrest, 2016), and new estimates on cost per incident (Romanosky, 2016). This research runs counter to common, and widely cited industry survey results. For example, the Ponemon Institute's 2017 report estimated $2 million per breach (Ponemon, 2017), while Romanosky's estimate is closer to $200,000. These lines of research provide important insights into the impacts of control failure but provide less insight into the contribution of compliance to the success or failure of the organization.

The review of the literature demonstrates that there is not a consensus on the ability of control frameworks to deliver consistent security outcomes. One theme that recurs in the literature is the challenge to implement and maintain the controls. Another is the difficulty to assess the controls in a reliable way to demonstrate a state of security,

and expected security outcomes, to third parties. I will examine this inconsistency in the literature through a case study of an organization and their implementation of information security control catalogues.

THEORETICAL BACKGROUND

After the 2007 financial crises, the accounting profession researched their own financial reporting compliance problem by examining the dynamics between auditors, financial institutions, and "governance, risk, and compliance" (GRC) methods. Michael Power's essay "The Risk Management of Nothing" (Power, 2009) focused on the concept of "risk appetite" and the inadequacies of metrics-driven Enterprise Risk Management (ERM) systems. He stated that ERM models should begin "to break free from regarding appetite solely as a 'thing' to be measured and to recognize it as a dynamic construction involving values and the situational experience of a multitude of organizational agents." Power uses the language and approach of complexity theory, as will be discussed later. Other research created models to try to correct the failures of the auditing standards that were intended to mitigate the causes of financial collapse. Some research described a Dempster-Shafer theory of belief systems for risk assessment (Mock, Sun, Srivastava, & Vasarhelyi, 2009). The use of Bayesian analysis and belief systems is at the heart of Douglas Hubbard's work on risk management (Hubbard, 2009). These approaches are focused on the broader issue of risk assessment, of which controls and compliance are only two components.

The complexity theory approach as described in Power's paper is the most appropriate for my research question. Complexity theory is a multidisciplinary approach to address the interactions between agents, and the potentially disproportionate impact of

their actions. First explored in the biological and physical sciences, complexity theory began to be applied to organizational behavior in the late 1990s, since traditional models did not have the power to explain why "organizations with nearly identical components have divergent results" (Grobman, 2005). Philip Anderson's description of complex adaptive systems (CAS) in organizations better explained the disparity between the traditional planning and outcomes (Anderson, 1999). Complexity theory has also been used to describe some organizational information security behavior (Burns, Posey, Courtney, Roberts, & Nanayakkara, 2017), and cyberwarfare (Phister, 2010).

Complexity theory was derived from observations in the natural sciences of self-organizing systems that do not appear to follow a single pattern. Examples include the behavior of bee and ant colonies, where individual insects operate together to achieve an objective without any central controlling structure. Concepts of self-similarity, chaos, and the "butterfly effect" fall under the larger study of complexity theory. In Complexity: A Guided Tour, Melanie Mitchell described the three principles of complex systems: complex collective behavior, signaling and information processing, and adaptation. (Mitchell, 2009). In complex systems, individual components, or agents, act according to a set of rules, or schema, with the agents' schema creating a reaction to the agents that surround it. The agents also communicate with each other, recognizing and processing the information signals sent from other agents. The system adapts to changes in the environment. These primary concepts contribute to phenomena in network effects, evolution of organizations, and power law, rather than normal distribution of effects.

A property of complex adaptive systems within an organization is the ability to create unpredictable results. Individual agents connect within the rules established by the organization, but also establish information shadow systems and develop their own schema to achieve their self-defined objectives. The shadow systems are non-linear, and "unexpected actions are likely to be produced" (Stacey, 1996). Instability, or chaos, in an organization can "amplify small changes in the environment, causing the instability necessary to transform an existing pattern of behavior into a new, more appropriate one" (Burnes, 2005).

In this paper, I use the principles of complex systems to describe the dynamic tensions between information security, compliance control catalogues, and disruptive events in the organization. These tensions may lead to a state where compliance catalogues of control would fail to meet their planned objectives of information security, and consequently reduce the ability of an organization to protect itself.

The compliance framework, including the catalogue of controls, contains elements from three complex systems interacting with each other, but with their own objectives and dynamics. These systems are self-similar, or fractal, as each resembles the other as agents follow the same set of schemas, in this instance control catalogues.

The highest level of compliance systems is at the governing or regulatory body that drafts and enforces the compliance rules. Examples include the PCI Council and the National Institute of Standards and Technology. The complex collective behavior is demonstrated in the rulemaking and enforcement processes, as the organization seeks to collect and process information on control implementations, as well as evaluations of

assets and threats, from its members. The PCI Council, for example, includes members from different participating organizations, while NIST seeks input from federal agencies and organizations when developing rules. These communications with other organizations include the second component of a complex system, information signaling and processing. The governing body distributes draft rules and holds meetings to discuss the proposed framework. Based on the communications from the members of the framework, the governing or regulatory body adapts, making changes to the control catalogues. Since changes to the catalogues require implementation by the regulated organizations, the governing bodies seek consensus from their member organizations, and the changes to the control catalogues occur at a rate much slower than the changes to technology or organizations. Nonetheless, these changes reflect the divergent paths in defining controls as illustrated above regarding password rules and demonstrate how the complex system property of similar objectives can lead to differing results.

At the next level is the organization which is both governed by these regulations and required to implement the control catalogues. The organization demonstrates complex collective behavior as it interacts with vendors, customers, regulators, and other business partners. The implementation of the control catalogues may impact how these collective behaviors occur, defining the terms and limits of these relationships. Organizations signal and process information through contract negotiations, public statements, and display of certifications. The Equifax displays of compliance certifications on its website, and in its quarterly filings with the SEC, illustrate this

property of a complex system. The organization also adapts to its environment, including compliance requirements as well as the changes in financial and stakeholder objectives.

The final complex system is at the level of individual teams within the organization. Although the information security team typically implements the controls required to comply with the compliance framework, this team of individuals must also collaborate with the other teams within the organization to accomplish their tasks. They signal and process information from organizational leadership regarding their progress and priorities. Changes to the organizational environment, including new business lines and changing stakeholder priorities, require the information security team to change and adapt their processes.

Information security systems by their nature interact with another complex system that behaves outside of the trust framework, but gives it meaning: the threat system. The threat system is defined as a system that attempts to breach the confidentiality, integrity, and availability of protected information assets. These threat systems are diverse in their composition, motivations, and methods. Threats to information systems include nation-state actors, large networks of organized criminals, and single opportunistic individuals. The threat system can operate within the organization as an "insider threat." Vendors, employees, contractors, and customers may all act as agents in the larger threat system.

How do these complex systems influence the relationship between control catalogues and security outcomes? The governing bodies develop the control catalogues in complex system separate from the organization, and the information security team that is required to deploy them. The catalogues are also separate from the complex system of

the threats seeking to penetrate the organization. The compliance framework and control catalogues can influence the ability and format of the information security team's communication within the organization. The security team's response to threats may be framed by their implementation of a catalogue of controls. In terms of complexity theory, the agents of the information security team are handed the schema developed by the trust framework and are expected to adapt to the systems of the organization and the threats. This dynamic may not produce the expected security outcomes since the schema/control catalogue may be implanted in the organization's systems without consideration of the existing environment. Even with a common set of rules, the initial conditions of each organization differ, and lead to divergent outcomes, and emergent random behavior. Complex systems are sensitive to initial conditions, and "the behavior of some simple, deterministic systems can be impossible, *even in principle*, to predict in the long term" (Mitchell, 2009). The catalogue of controls may inhibit the organization's ability to evolve in response to the threat information signals and environment.

METHODOLOGY

This research uses a case study approach to analyze the complex systems of a trust framework within an organization and the organization's information security team. The research uses the three properties of a complex system: complex behavior, information communication, and adaptability. The case study identifies the impact of the control catalogue on the ability of each system to meet its goal of improving security outcomes. I present the case study as the organization changes strategy, leadership, regulatory mandate, and IT investment. I selected the case study approach for its ability to examine the relationships between the regulator, the organization's leadership, and the information security team in sufficient detail to identify the dynamics of the complex adaptive systems.

I selected the case study organization due to the ability to examine the changes to leadership and strategy. Individuals with extensive knowledge of the history of the organization were available for interviews. The organization permitted this research on the condition that neither the organization nor its industry be identified. This paper refers to the organization as YZ Corporation, and its regulator as the Department. After the narrative of the history of the organization, I describe the methods of information collected. I use the information to identify the properties of the complex system, how it signals and processes information, and how it adapts to its environment. The information will also provide measures of the organization's security outcomes.

Background on Case Study – YZ Corporation

YZ Corporation is a non-profit organization, established in the 1980s to serve a federal program. As YZ grew, it increased revenue through expanding its area of service and innovating within a set of federal and state regulations. By 2008, YZ employed over 700 people with revenue over expenses of $80 million. YZ's customers included both institutions and individuals. YZ's primary business required it to collect and maintain several million records containing the non-public personal information (NPI) of individuals.

YZ adopted e-commerce early, using the internet to facilitate its social mission, and to accelerate financial transactions and data transfers with institutional partners. Beginning in 1995, YZ recruited a large team of developers to integrate e-commerce and data exchanges with existing mainframe processes, including the development of standards in coordination with partner institutions. The organization developed a Project Management Office and tied corporate compensation to the completion of strategic projects. From 1995 to 2000, the number of developers grew to nearly 25% of the organization, with approximately one third of them contractors. The information security function remained static, consisting of three individuals who reported to an IT infrastructure manager. The information security team administered access controls, configured the firewall, and maintained the business contingency/disaster recovery plans. YZ's primary IT compliance obligation consisted of adherence to Gramm-Leach-Bliley Act (GLBA) controls as defined by the Federal Trade Commission. The information

security team was responsible for completing, evaluating, and exchanging GLBA questionnaires from business partners.

In 2006, YZ contracted with a system integrator to assist in a data management project. During the testing phase of the project, a developer for the system integrator lost a device that contained data to be used for system testing. The loss of the device was a significant event, since the "test data" was over one million records of production non-public personal information representing current and past customers. Once notified of the incident, YZ responded by mailing notifications to the impacted individuals, establishing a call center to respond to their questions, and creating a website to communicate updated information on the data loss. YZ hired a law firm to assist in the response and initiated legal action against the systems integrator. The news of the data breach was published on the front page of the local paper serving YZ's community, as well as state and nationwide media. YZ maintained communications with the Department throughout the process. The Department required no additional actions other than those YZ performed. Although some business partners performed additional due diligence on YZ's information security practices, no business relationships were lost as a direct result of the data breach.

In 2007, YZ contracted a security firm to conduct a penetration test of its network. The test identified several non-critical vulnerabilities, which the information security team remediated. Also, in 2007, YZ created the position of Information Security Officer, and increased the number of security staff from three to five. The Information Security Officer developed a security policy and procedure framework using ISO security

standards and NIST's FISMA guidance as a baseline. Although YZ was not required to comply with FISMA, the Information Security Officer selected NIST Risk Management Framework due to YZ's connection to the federal government, and the potential to enable YZ to compete for future federal contracts. According to the Head of IT, YZ's "approach to the FISMA control catalogue was that it was a set of good practices we could pick from" and YZ "implemented the controls we felt best improved security."

From 2007 to 2010 YZ expanded into new territories, providing new internet enabled services to its institutional customers. To support the innovation, YZ focused on extensive software and enterprise architecture projects. With significant reserves and growing revenue, YZ structured its incentive bonus system on the timely delivery of services to customers, rather than the cost to build the services.

In 2009, YZ wanted to be prepared to bid on a federal contract and sought to hire a consulting firm to identify gaps between YZ's existing security controls and those required by FISMA. In October 2009, YZ management requested $170,000 from YZ's board of directors, framing the engagement as a "compliance" effort. In the presentation to the board, management described the FISMA compliance assurance as "critical to ensuring YZ's systems are accredited for future competitive offerings." YZ contracted with a large international consulting firm to conduct the assessment. The consulting firm presented their results to management in September 2010. The consultants' assessment recommended that YZ embark on a larger project that would include establishing a Role Based Access Control (RBAC) system, designing a new network architecture for the internet-facing environments and documenting existing information security processes in

a manner compliant with NIST standards. The consulting team would develop a Plan of Actions and Milestones (POAM) that would identify unremediated gaps between YZ's controls and controls required by FISMA. The consultants estimated the cost of this engagement to be $1.5 million.

During the engagement, the consulting firm expanded the scope to address their discovery that YZ continued to use production NPI in the test environment. The issue of production data in the test environment was a proximal cause of YZ's 2006 data breach. YZ paid a total of $2.25 million to the consultants. The consulting firm concluded its engagement in August 2011, delivering a POAM, information security policies and procedures derived from the consulting firm's templates, a spreadsheet-based RBAC, and the deployment of intrusion detection, intrusion prevention, and data leak prevention products.

In 2010, federal legislation was passed that would lead to a slow decline, and eventual end of YZ's primary revenue source. YZ management developed a strategy to identify alternative sources of revenue and placed its primary focus on bidding for a federal contract. To prepare for the bid, YZ management began a renewed focus on implementing and documenting FISMA controls.

In July 2012, YZ conducted its first lay-off of personnel, primarily employees that staffed functions made obsolete by the 2010 federal legislation.

YZ's Project Management Office continued to address the POAM items. Management identified the "POAM Project" as a high priority and used its on-time completion to calculate the level of year-end bonuses for corporate management and

staff. Management allocated and prioritized resources to address the POAM items, while other IT areas tried to reclassify languishing infrastructure upgrade efforts as necessary to achieve FISMA compliance. The initial POAM Project was completed in September 2013. In December 2013, the Information Security Officer found employment opportunities with another organization and management filled the position with senior member of the information security team.

In January 2014, the information security team had 8 members in three areas: Security Operations Center (event monitoring and incident response), Access Control (maintaining the RBAC and managing access to internal and external systems), and Program Management (developing and maintaining policies and standards). The security team changed its reporting relationship, so the Information Security Officer now reported directly to the senior executive in charge of IT. IT management transferred the maintenance of the firewall and newly acquired security devices to the network support group, although the information security team remained responsible for the rules and configuration of these devices to maintain separation of duties.

In March 2015, with no federal contract or alternative revenue stream forthcoming, the board of directors replaced the CEO with another YZ executive. The new CEO designed a strategy to develop a new revenue generating business, identify potential organizations for acquisition, and create new alliances with other organizations within YZ's primary business. The CEO restructured the organization in April 2015 to align the organization with new strategic goals and reduce infrastructure costs. The cost reductions included significant layoffs, primarily of IT staff. The restructure eliminated

the project management office, application development, and enterprise architecture departments, with significant cuts to personnel in infrastructure and help desk support. The restructure reduced the information security team from 8 to 4 by layoffs, with two additional team members resigning in reaction to the cuts. By October 2015, the remaining team consisted of two analysts and the Information Security Officer. IT was no longer represented in senior leadership but reported to the new CFO. To further reduce on-premise infrastructure costs, IT developed a strategy of leveraging cloud services whenever possible for replacement systems and storage. Corporate goals and bonus calculations were now focused on cost reduction, rather than project completion.

The primary reason for the reduction of the Information Security team was the organization's pivot from focusing on a federal contract to seeking other sources of revenue. Since the information security team presented their primary value as FISMA compliance, management saw no need to retain the staff since the new business opportunities would not require FISMA. This action was part of a broader strategy based on the assumption that YZ had significantly overspent on compliance activities. According to the Information Security Officer, the new CFO characterized the compliance program as "gold plated." The Head of IT described the change between the two CEO approaches from "automatic approval for budget if it went to compliance" to "every dollar spent on compliance was challenged."

Meanwhile, the Department began to conduct assessments of third party risk, based on recommendations from their Inspector General. The Department's Inspector General reported weaknesses in the Department's information security as a "top

management challenge" since 2011. In March 2015, the Department asked YZ and similar institutions to complete an information security self-assessment that closely mirrored the controls identified in the FISMA control catalogue. In July 2015, just three months after YZ laid off most of their security staff, the Department issued a letter that required YZ and similar institutions to comply with FISMA standards as a demonstration of their administrative capability. The Department requested YZ contract with a third party to conduct an independent assessment of YZ's implementation of FISMA's security controls. YZ's information security team and representatives of the similar institutions held periodic conference calls with the Department to determine the scope and depth of the Department's expectations. YZ hired a contractor to assist with documentation and later perform an assessment of YZ's compliance with FISMA. The initial assessment was performed in the summer of 2016, identifying several areas for remediation. The CFO and Head of IT allocated resources to address the outstanding issues identified by the third-party assessor, primarily focusing on vulnerability management of the legacy system. A second assessment by the same firm was conducted in 2017. The Information Security Officer communicated to the Department when the assessments were complete, but the Department did not request copies of the reports.

As part of its new strategy announced in April 2015, YZ planned for a division responsible for new revenue, which I reference as "New Division." YZ created New Division in 2016 and staffed it with leaders from outside the organization. In the summer of 2016, New Division hired a sales team, and aggressively marketed its services in a competitive market. The Head of Internal Audit related that management and the board

of directors anticipated that New Division "would act like a start-up, but with the resources of YZ." As YZ's legacy revenue decreased, YZ planned that New Division's revenue would replace it. YZ provided services to New Division through a shared services agreement. The shared services included IT and information security, as well as accounting, legal and human resources.

New Division identified information compliance programs it would need to compete in the marketplace. YZ's Information Security Officer said that New Division was "making commitments that included compliance with HIPAA, PCI-DSS, ISO, as well as talking about a SOC2 assessment. I don't think they knew what this compliance would cost." The Information Security Officer made an initial review of the information security compliance requirements the New Division would need to implement and document. According to the Head of IT, "by the time we started looking at what New Division wanted in terms of compliance, we were looking at over 900 controls. Do we really need to implement these 900 plus controls?" In early 2017, the Head of IT contracted with a local consulting firm to help in developing an information security compliance framework to address all YZ's business lines, including New Division. The local consulting firm offered their own consolidated control framework, including policies and procedures, that would map to these 900 controls. In the summer of 2017, the Head of IT presented the policies and procedures to different business areas to solicit opinions and obtain commitment to the new control framework. The Head of Internal Audit commented that, although the framework was comprehensive, it would require some additional customization to conform to YZ's business processes.

By March 2017, New Division provided services to four customers, with an operations staff of twelve and sales staff of five. The technology YZ supported for New Division was a mix of both on-premise and cloud systems. No independent third party had evaluated the security of New Division systems by the end of 2017, but vendor management teams from New Division customers had made on-site visits.

Table 1 YZ Corporation Timeline

2006	May	Data breach
2007		Position of Information Security Officer created
2008		
2009	October	FISMA consulting project approved by board of directors
2010		Legislation ends YZ's program Consultants begin FISMA gap assessment FISMA project begins
2011	August	Consultants complete FISMA gap assessment
2012	April	First layoff
2013	July	First security awareness quiz administered
	September	First FISMA project completed
	December	Change in Information Security Officers
2014		
2015	April	New leadership & strategy, with plans for New Division Reduction in force, primarily in IT
	July	Department makes FISMA required for YZ
2016		New Division begins operations
	September	First FISMA assessment report issued
2017	September	Second FISMA assessment report issued

Data Collection Methods

Information on YZ's control catalogue implementation and security outcomes was collected by the following methods.

Interviews:

I interviewed the following employees of YZ Corporation to better understand the dynamics between the information security compliance and outcomes as YZ underwent organizational changes. I include the results of these interviews to add perspective and background to the quantitative and qualitative results.

Table 2 Interviews with YZ employees

Title	Background	Interview Duration	Topics of Interview
Head of IT Division	Former head of application development at YZ. Promoted to head of IT division in 2015 reorganization. Over 10 years with YZ.	One one-hour, one half-hour session.	The history of YZ Corporation, and its approach to information security. The approaches to information security compliance at YZ. YZ's approach to information security risk. How changes in budget, staffing, and leadership influenced the ability of YZ to implement compliance control catalogues and manage security outcomes. YZ's cloud strategy.
Head of Information Security	Promoted to head of security from security engineer in December 2013. With YZ from October 2011 to until December 2017.	One-hour session	Relationship between Information Security and other organizational units. Relationship between compliance and security. Impact on reduced resources in meeting security objectives. Impact of assessments (penetration tests, FISMA assessments). Relationship with the Department.
Security Analyst	Employed by YZ for over 25 years. Primary responsibilities in information security compliance and managing assessment engagements.	Two 30-minute sessions	Relationship between Information Security and other organizational units. Compliance and security. Impact on reduced resources in meeting security objectives. Impact of assessments.
Head of Internal Audit	Led YZ's internal audit function from August 2015 to December 2017.	Two one-hour sessions	Approach of board of directors to information security. Background on internal audits of information security.
Human Resources Trainer	Administers the security awareness quiz.	One half hour session	Collection of quiz data, description of process.

YZ provided me with documents and reports maintained by the organization that illustrate their information security and compliance programs. These records were created, formatted, and retained to support an ongoing business. I was unable to obtain some records that would illustrate YZ's security and compliance programs, or records for a period that would better illustrate trends due to the practical demands of an ongoing business.

This report uses the following information to assess YZ's security and compliance outcomes, as well as variables that contribute to these outcomes.

Penetration Test Reports:

I collected and reviewed the results of the penetration tests of YZ's internet accessible systems from 2012 to 2017. The external penetration testing firm annually conducted two tests, one web and one external, and issued two reports. The scope for each test did not change from one year to the next, however the tools and techniques used by the testing firm changed to align with evolving threats. The web test identified vulnerabilities on YZ's single web application for external customers. The external test identified vulnerabilities in systems identified by the 128 public network addresses owned by YZ. The firm prioritized the results, with the highest priority assigned to the vulnerabilities the penetration test team used to gain unauthorized access to YZ information assets. The firm prioritized the other results according to security industry standards (CVSS, OWASP Top Ten).

These tests were intended to simulate actual attacks on YZ's systems. A decrease in the number and severity of reported findings reflect better security outcomes, and

reflect YZ's ability to maintain, patch, and configure the systems at a level consistent with the level of external threats.

External FISMA Assessments:

I analyzed the reports created by the external FISMA assessors of YZ's environment. The assessors issued reports in September 2016 and September 2017. The 2016 assessment included a review of all 262 controls listed in the FISMA control catalogue (NIST Special Publication 800-53, Appendix F). The 2017 assessment covered 143 controls, including controls considered "critical" by the assessor, and one third of the remaining controls. The assessor plans to rotate the non-critical controls each year, so a full assessment of all controls would occur over a three-year period. The Department's FISMA requirements for YZ did not require an official Authority to Operate (ATO), so the Department did not receive the results and an ATO opinion was not issued. The assessment firm presented the results ranked on a High/Medium/Low qualitative scale. The assessment reports included vulnerability scans of YZ's FISMA-scoped systems. The reports provide an indicator of YZ's compliance with the FISMA regulations as required by the Department, and as assessed by a third party.

A decrease in the number and severity of action items identified in the report will indicate improving security compliance outcomes.

Internal Audit Reports:

I reviewed the reports written by YZ's internal audit team with a scope that included information security processes from January 2010 to September 2017. The internal audit director selected areas to be audited based on an annual risk assessment that

included input from YZ management and board. The reports presented findings, recommendations, and management action plans. The findings from 2015 to 2017 ranked the impact of the findings on a qualitative scale.

The internal audit reports assessed information security controls, including policies, procedures, and processes. Recurring findings indicate a higher risk for poor security outcomes. The internal audit reports also assessed systems that were not in the scope of the FISMA or penetration test engagements, providing a broader perspective on the information security outcomes across YZ's operations.

Financial records:

Financial information on YZ's annual revenue and expenses were collected from YZ's annual audited financial statements from 2010 to 2017. YZ's fiscal year runs from October 1 to September 30. I collected the operating margin data from quarterly reports to the YZ board of directors. YZ's uses an adjusted operating margin to communicate corporate performance to the board, and to calculate annual bonuses. YZ adjusts the number to exclude expenses and revenue not related to corporate performance.

The financial information is an indicator of the health of YZ, and its ability to support its operations. Financial measures can indicate the amount of energy available to the organization as a complex adaptive system.

Head count:

I collected the number of employees at YZ corporation from dashboard reports provided to the board of directors by YZ management. YZ's human resources department reported the head count of the organization as calculated at the end of the

fiscal year. The Information Security Officer provided the head count of the information security team.

The changes in head count of YZ and the security team illustrate the resources available to generate revenue, secure YZ's assets, and implement security controls.

Minutes of Board of Directors meetings:

Until 2015, YZ held quarterly board of directors meeting, usually occurring in March, June, September, and December. The board agendas focused on planning in the March and June meetings, the budget in September, and corporate goals and financial statements in December. I was able to review the December board books for 2011, 2012, 2013 and 2014 based on the access I was granted by YZ. The December board books contained the agenda for the December meeting, audited annual financial statements, minutes from the September meeting, and supporting materials on corporate performance. In 2015 YZ changed the method they used to prepare the board documents and held the meetings on a different schedule. I was able to review the December 2015, February 2016, December 2016, February 2017, and May 2017 board materials. I reviewed all materials to identify discussions of information security and corporate strategy. The Head of Internal Audit and Head of IT provided additional background information on the board meetings that discussed information security (August 2009, February 2016, February 2017, May 2017). The board minutes and documents provide insight into the priorities of compliance and information security, including their reasoning behind investments in information security. These materials document how

YZ's management of information security is communicated and signaled between management and the board.

Results of information security awareness quiz:

I collected data from the software used to administer the security awareness quiz from its 2014 to 2017. The data includes a record for each employee that completed the test, and the number of incorrect responses to each question. The number of tests administered do not match corporate head count numbers due to employee turnover. According the HR Trainer, YZ contacts employees and their supervisors until all quizzes are complete. YZ first administered the quiz in 2014. The quiz data measures YZ employee's information security level of awareness, which may represent the ability of the information security team to communicate security and compliance priorities with the rest of the corporation.

Privacy and security incident reports:

YZ records information on potential privacy and security incident reports in workflow management software. The available 103 records began with incidents entered in the system in October 2011 with the last record dated August 2017. The data include the source of the report, a brief description of the incident, and information on its disposition. The sources of the incident reports include submissions from a corporate intranet form, e-mails sent directly to the Information Security Officer or General Counsel, and entries created by the Information Security Officer or General Counsel, based on information independently obtained.

The incident information provides insight into how the employees exercise their compliance with YZ policy to report incidents, as well as how changes in the corporate complex adaptive system may impact the frequency and type of incident reported.

Virus, Spam, and Phishing Reports:

YZ's trouble ticket system records all employee reported technical problems that was not be resolved by support in the first contact. I selected virus, spam, and phishing items that were logged to the e-mail, security, and desktop categories. The data include when the incident occurred, who reported it, a brief description of the incident, the team assigned to resolve it, and when the team resolved the incident. YZ corporation collected this information from October 2011 to August 2016. Like the incident reports, these data reflect the engagement of YZ employees in protecting YZ information assets, and compliance with policy regarding reporting incidents.

Annual Information Technology Budgets

With a fiscal year that begins on October 1, YZ departments plan their budgets in July and August, based on the strategy and objectives established in June board planning meetings. Management consolidates the budgets and present the annual budget to the board of directors in the September meeting. I obtained the budget total for information technology department from 2010 to 2017. The budget includes the anticipated annual costs for personnel, software, hardware, and information technology projects. YZ places all software costs in the information technology budget. The information technology budget also includes cloud services. The budget information I reviewed did not separate the items based on their function or role within IT. For example, I was unable to

determine the amount budgeted each year for information security, however the IT budget included all information security functions except for training, awareness, and physical security.

The budget is an expression of YZ's IT strategy for the next year. Changes to the budget, either up or down, reflect YZ's plan to invest in technology, or its desire to reduce cost.

IT Intensity

IT intensity is a calculated variable representing the ratio of IT budget to total revenue for a fiscal year. This measure normalizes the IT budget over time to determine the year to year investment in IT. The investment in IT will correspond to the investments in information security and compliance. IT intensity represents the changes to the level of energy YZ allocates to information security.

Costs of Cloud Implementation

Beginning in October 2014, YZ's IT strategy included an increased focus on leveraging cloud-based systems to support business functions while reducing support and infrastructure costs. I collected financial information on the cost to YZ of their investments in Software as a Service (SaaS) and other cloud-based systems from January 2010 to December 2017. The deployment of the cloud systems may impact the support, security, and compliance burden on YZ's IT team, as well as YZ's overall security outcomes.

I discuss the results framed within the three concepts of complex systems: complex behavior, information signaling, and adaptation. The security outcomes rely on

the penetration test results and internal audit assessments. The level of control catalogue implementation will rely on the FISMA compliance assessments. IT intensity, the employee incident reports, and other financial and organizational results will place these variables within the context of a complex system to aid the interpretation of the outcomes. The results cover a period when YZ experienced several significant changes in corporate leadership, strategic direction, and regulatory requirements.

RESULTS

The results are framed in the context of complexity theory to help determine the dynamics between the control catalogue implementation and the security outcomes. Some results may apply to more than one complexity principle.

Table 3 Organization of Results

Complexity principles	**Properties**	**Organization**	**Security Team**	**Outcomes**
Complex behavior	Rules and schema. Individual agent Reactions to surrounding agents	Organization headcount	Privacy and Security incidents Virus, Spam, and Phishing Incident Security Team headcount	
Information Signaling	Creating and transmitting signals Receiving signals Processing information	Board meeting minutes Internal audits	Security awareness quiz	FISMA Assessment
Adaptation	Changing schema to optimize performance "Evolution to the edge of chaos" Gathering energy	Revenue, Expense, and Operating Margin Cloud system costs IT Intensity		Penetration test results

Tables 4 and 5 present the raw data for the information security and financial measures. Figure 1 provides a visualization of the normalized data.

Table 4 Information Security Variables

	2011	2012	2013	2014	2015	2016	2017
Corporate Head Count			634	597	456	405	364
Security Headcount			7	6	3	3	3
Internal Audit Head Count	6	6	6	6	3	3	3
Employee Reported Incidents			24	38	10	20	11
Spam, Virus, and Phishing Reports (SVP)	4	7	6	9	12	5	
Total Completed Awareness Quizzes			695	703	585	601	470
Perfect Scores on Awareness Quiz			196	255	205	219	170
Pentest findings (all)			76	89	95	107	80

Table 5 Financial Measures in Thousands of Dollars

	2010	2011	2012	2013	2014	2015	2016	2017
IT Budget		28,519	27,654	26,621	25,742	24,404	15,287	14,505
Revenue	190,246	115,206	206,206	104,384	148,962	152,169	265,217	122,173
Expenses	145,211	95,588	40,144	127,913	98,420	71,192	62,946	59,714
Cloud cost	19	42	31	27	21	144	146	330
Adjusted Operating Margin	43.24	35.12	40.46	43.69	41.31	44.8	43.9	51.21

Figure 1 Graph of Normalized Values

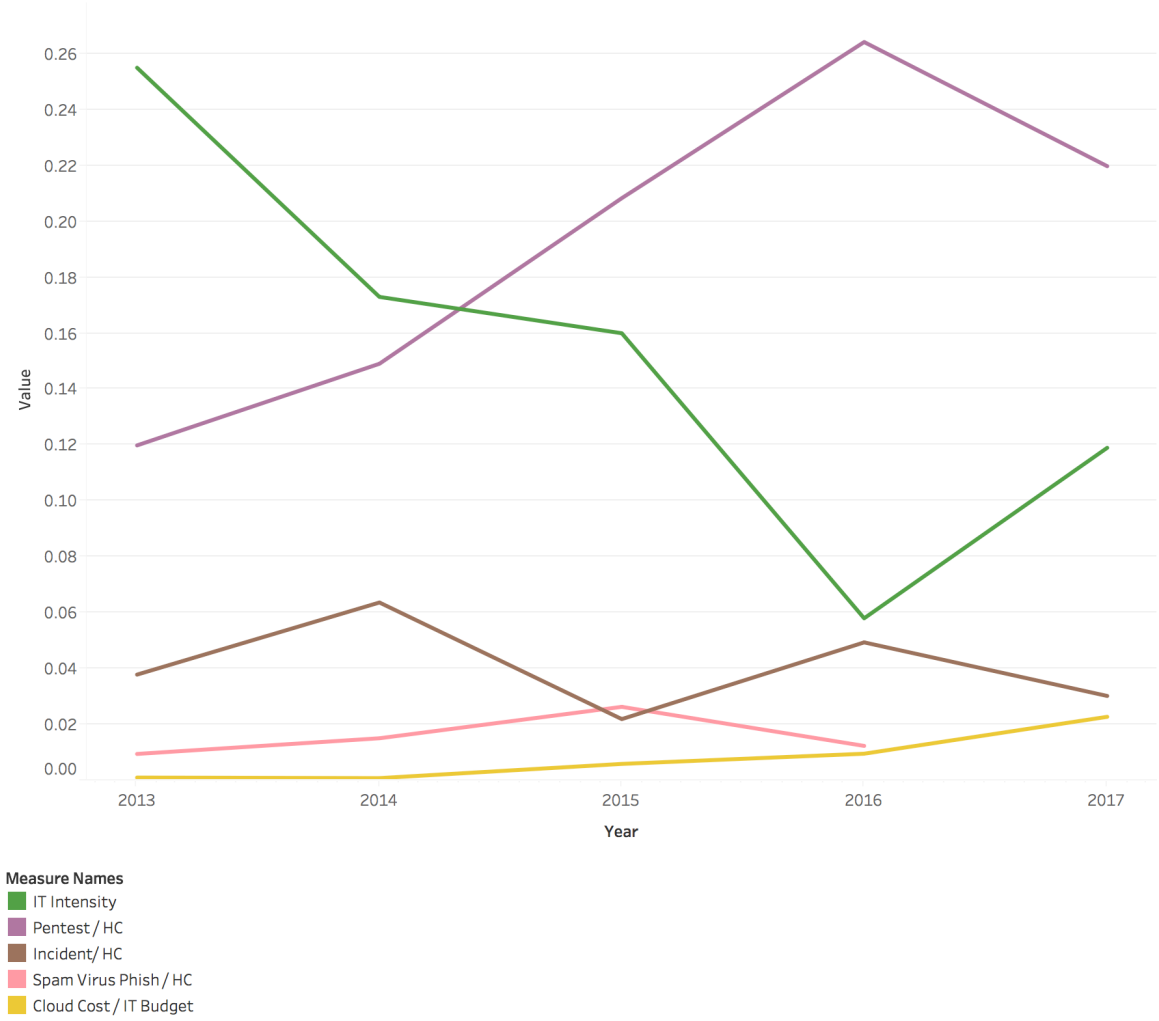


Table 6 Values of Normalized Results

	2013	2014	2015	2016	2017
IT Intensity	0.2550	0.1730	0.1600	0.0580	0.1190
Pentest / Headcount	0.1199	0.1491	0.2083	0.2642	0.2198
Incident/ Headcount	0.0379	0.0637	0.0219	0.0494	0.0302
Spam Virus Phish / Headcount	0.0095	0.0151	0.0263	0.0123	n/a
Cloud Cost / IT Budget	0.0010	0.0008	0.0059	0.0096	0.0228

IT Investment in Control Catalogue Implementation

The value of IT intensity is the percentage of revenue dedicated to IT. I use this variable to represent YZ's investment in the control catalogue. The lowest point of investment in control catalogue implementation is 2016, the same year YZ underwent its first initial FISMA assessment. The level of intensity decreased from just over 25% in 2013 to slightly more than 5% in 2016, recovering to 12% in 2017. The 2016 spike in revenue contributed to the low that year, but the downward trend reflects YZ's shifting priorities. Although YZ's IT team had fewer employees to support, the team still had to maintain the static legacy system responsible for 90% of YZ's revenue. In addition, the IT team was also responsible for deploying and provisioning systems for the New Division. IT budget contains all corporate software and hardware costs, including cloud services.

Of the 262 FISMA controls for YZ's environment, IT was responsible for implementing 231. YZ's human resources and building management departments implemented and managed the remaining 31 controls, representing 12% of the catalogue. These 31 controls represented the Awareness and Training, Personnel Security, and

Physical and Environmental Protection control families. The information security team also led the efforts for New Division information security compliance.

Penetration Test

Table 7 Penetration Test Details

	2012	2013	2014	2015	2016	2017
External Critical and High Findings	0	0	2	1	6	3
Web Critical and High Findings	0	2	1	1	3	3
All Critical and High Findings	0	2	3	2	9	6
All Web Findings	12	5	43	46	54	42
All External Findings	19	25	46	49	53	38
All Penetration Test Findings	31	6	89	95	107	80

The number of penetration test findings reached a peak in 2016, the same year the investment in IT controls reached its lowest value. The firm tested the same web application each year. YZ moved three external hosts to a cloud provider in 2016, but the report did not reflect a change in scope, since the firm tested the same 128 public IP addresses. The other systems YZ moved to cloud environments were not accessible from the internet and were not within scope of the penetration tests.

The increase in web application findings in 2016 may reflect the aging of the legacy customer portal. Until April 2015, YZ's Project Management Office developed and maintained the web application with the rest of the legacy system. After the

development stopped, a significantly reduced support staff was responsible for maintaining the web application infrastructure. The Information Security Officer commented that "patching is hard because the business doesn't want any disruptions" and "scheduling the patches is difficult, especially with the legacy applications." The Information Security Officer also described the challenge in convincing the IT support team of the priority of security changes.

FISMA Assessment Results

With only two reports with different scopes and reporting formats, I will analyze the FISMA assessment results both quantitatively and qualitatively. After the Department recommended a third-party FISMA assessment in July 2015, YZ hired an assessment firm to prepare YZ's policies, procedures, and standards in a FISMA compliant format. A different team from the same firm conducted the 2016 assessment, as well as the 2017 annual assessment. As mentioned in the narrative, the Department did not request copies of either report, but continued to rely on annual self-assessments.

The first assessment was conducted in the summer of 2016. The firm conducted the assessment following the NIST assessment guide (SP 800-53A). The firm reduced the scope of the 2017 assessment to only include "key controls" that would be assessed annually, and one third of the remaining controls. The remaining controls would be rotated every year, so a complete assessment of all controls would be complete over three years. The firm also changed the method they reported risks. These changes presented

challenges to identify differences in security outcomes. Table 8 presents the detailed results from the two assessments.

Table 8 FISMA Assessment Results

	2016 Assessment	2016 Vulnerability Count	Ratio of Controls Assessed to Risks	2017 Assessment	Ratio of Controls Assessed to Risks	2017 Vulnerability Count
Controls reviewed	262			143		
Risks – High	23	23	9%	1	0.6%	264
Risks - Medium	15	7	6%	4	3 %	218
Risks – Low	14	0	5%	3	2%	101
All Risks	52	30	20%	8	5%	583
POAM Items	54			8		
Repeat POAM Items	N/A			5		

The scope of the 2016 assessment included all 262 FISMA controls required for a medium risk environment. The reported risks represented the number of instances of non-compliant control. Some POAM items referenced multiple controls, and some controls were listed on multiple POAM items. The assessor included 30 unresolved vulnerabilities identified by YZ's vulnerability scanner as risk and POAM items in the 2016 assessment.

The assessor changed the reporting format for risks and POAM items between 2016 and 2017. In 2016 the assessor included a single risk for vulnerability management but included individual POAM items to remediate each vulnerability. In 2017, the

assessor reported the scan results alongside the risks as equivalent items in an overview of the organization's risk, and as individual POAM items. This list was based on the scan results YZ provided to the assessor that included systems that were not in scope.

The information security team challenged the assessor's method of reporting risk, the scope of the assessment, and the inclusion of each outstanding vulnerability in the 2017 assessment, but the assessor did not change its report. The Head of IT said the assessors "just took our scan results and spit them back at us." Based on an interview with the Information Security Officer, a review of the assessment work papers, and a review of the 2017 internal audit analysis, the root cause of the numerous outstanding vulnerabilities was the inclusion of systems outside the scope of the assessment. According to the Security Analyst, the assessor reported vulnerabilities on isolated network segments that had a low probability of exploitation. Other vulnerabilities were false positives. The Security Analyst added that communication with the assessors was not optimal, as the security team was also working on high priority project for the New Division. He added that patching the vulnerabilities of the legacy web application continued to challenge the IT team, but he felt sufficient compensating controls reduced the risk the vulnerabilities posed.

The assessment also presented the results in a taxonomically ambiguous fashion. The report presented "risks" alongside "vulnerabilities" as units of equivalent value, adding them together for an overall risk score. Although YZ may have been vulnerable due to their capacity to remediate legacy applications, the report overstated the magnitude

of the risk. The Head of IT stated that he was uncertain if the same firm will return to perform the assessment in 2018.

Internal Assessments

YZ's internal audit department provided independent assessments of YZ's operations, including privacy and information security. The head of internal audit reports to the audit committee chair of YZ's board of directors. Between 2010 and 2012, the internal audit department consisted of three operations auditors and two IT auditors in addition to the head of the audit department. The audit team conducted annual risk assessments using qualitative methods, primarily relying on input from surveys and interviews with the board, management, and key staff. The head of internal audit submits the risk assessment and audit plan to the audit committee. Audit staff usually participated in IT project team meetings and provided continuous auditing for selected operational and IT processes until 2014.

In late 2014, the head of internal audit left YZ employment, followed soon afterwards by other staff. When the replacement head of internal audit was hired in fall 2015, only two of the six auditors remained. The audit department consists of the head of internal audit, an operational auditor, and an IT auditor.

Full scope audits were between 400 and 600 hours long and took four to six months to complete. Limited scope audits were between 200 and 300 hours, lasting two to three months. Consulting projects were scoped under an engagement memorandum at the request of management and were less than 250 hours throughout the fiscal year.

Table 9 Internal Audit Assessments

Date	Type	Title	Findings
September 2010	Full scope	Information Security	The information security team had not yet implemented processes and procedures for implementing recommendations from the third-party consulting engagement.
October 2012	Consulting Project	Role Based Access Control (RBAC)	The audit team tested the RBAC to the RBAC spreadsheet accuracy.
January 2013	Limited scope	POAM Progress	The security team had not updated and maintained the policies, procedures, and processes. The report recommended the policies and procedures be updated to reflect current security processes and technology, and an annual review be implemented.
February 2016	Full scope	Network Security	The report included two minor findings related to maintenance of system inventory and incident response process documentation.
September 2016	Full scope	Cyber Risk and Security (non-FISMA systems)	The report included three medium impact findings: risk assessment of cloud services, secure configuration of cloud services, and data leak prevention configuration.
November 2017	Consulting Project	Security Review Update	Internal audit issued this memorandum to report on vulnerability management and the second FISMA assessment.

The audit results reflect the shift in YZ's security team's approach to implementation of the FISMA control catalogue. The September 2010 and January 2013 audits reported findings that identified the incomplete implementation of the consultants'

recommendations. The information security team had not maintained the draft FISMA compliant policies and had not communicated them to the organization at large. As a result, the policies and procedures began to diverge from organizational practices. The consulting project in 2013 provided the information security team assurance that their implementation of the process designed by the consultants worked as intended.

The 2015 audit on network security found only minor issues, and its scope focused on change management and network segmentation. The September 2016 Cyber Risk and Security audit was performed at the request of the board of directors. The audit scope was complementary to the initial FISMA assessment, excluding the legacy system being evaluated by the external assessors. The primary issues identified reflected YZ's strategy to use cloud services for new and replacement systems. The business areas acquired cloud systems without the information security team providing the risk assessment and access control assistance. According to YZ policy, a business unit must conduct an information security risk assessment before acquiring a new system. The information security team reviews and recommends mitigation strategies if necessary. The audit reported that several business areas completed the risk assessments after the contract was signed. One risk assessment was blank, with a note from the business area stating that since it was not a FISMA system, a risk assessment was not required. The audit also identified issues with the minimal effectiveness of the data leak prevention (DLP) tool. YZ deployed the DLP as part of the consultant's engagement, but the product was no longer supported by the vendor. The security analyst trained on configuring the tool left YZ in April 2015 as part of the reduction in force.

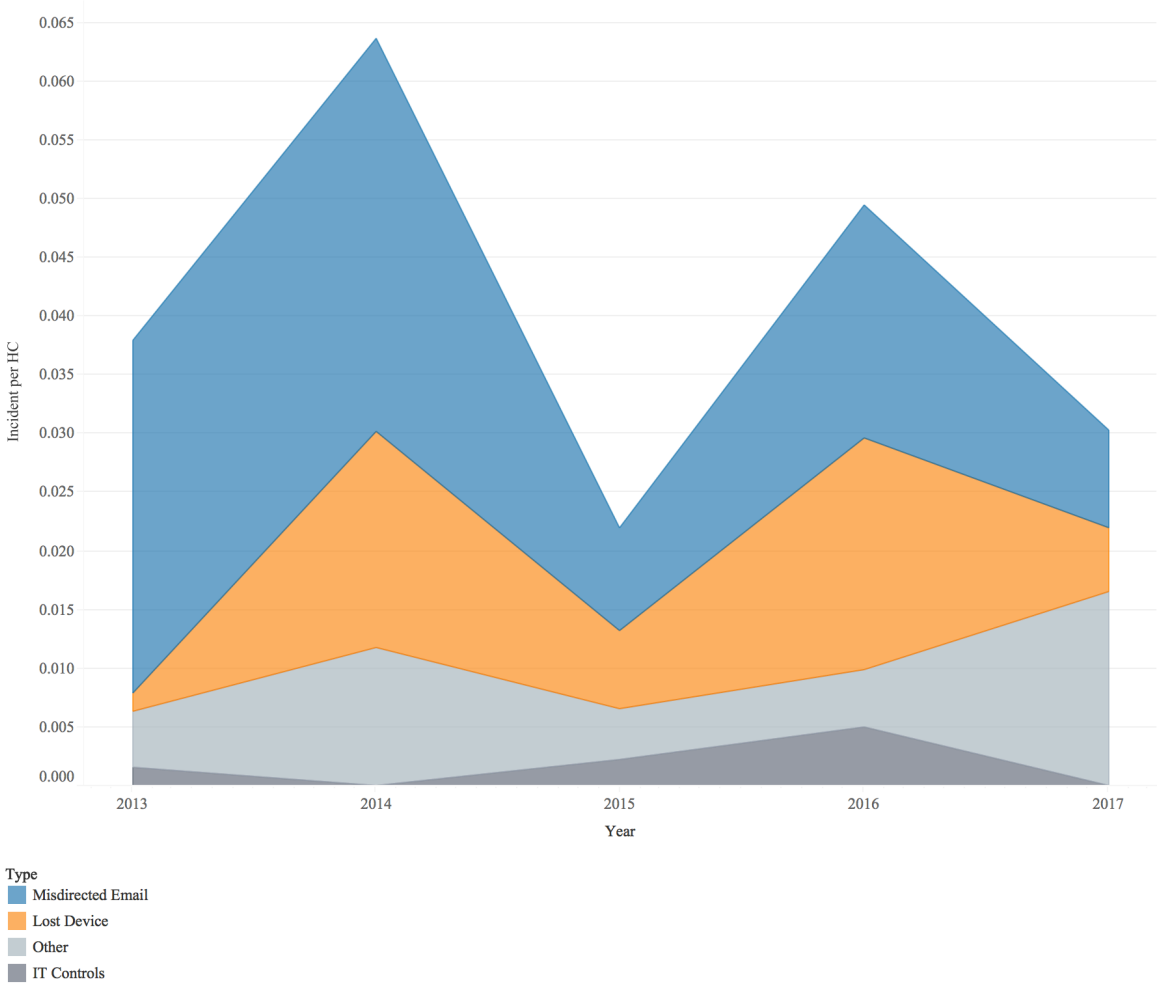
Privacy and Security Incidents

YZ policy requires employees to report potential security and privacy incidents through a form published on the corporate intranet. Table 10 represents the type of incident by year, and Figure 2 charts the incidents per head count by type from 2013 to 2017.

Table 10 Privacy and Security Incidents by Type

	2013	2014	2015	2016	2017	Percent of Total
Misdirected Email	19	20	4	8	3	52%
Lost Device	1	11	3	8	2	24%
Other	3	7	2	2	6	19%
IT/FISMA control related	1	0	1	2	0	4%

Figure 2 Incident Data by Type Normalized by Headcount 2013-2017



The incidents are divided into four types. *Misdirected Email* incidents represent events where an employee reports an error in the receipt or delivery of email, including correspondence to customers and marketing emails. These reports include incidents that may be a violation of regulations not related to information security. Policy requires employees to report lost phones and two-factor authentication tokens, which are represented in the *Lost Device* category. The response to lost device reports is the

deactivation of the device by the information security team. The four incidents in the *IT Controls* category map directly to a control in the FISMA catalogue, one physical control, one application control, and two involving malwares. The *Other* category records the incidents involving telephone and fax communications, issues with vendors, and other incidents that do not fit another category. The department of YZ that reported the most incidents was the department with direct contact with individual customers with 66% of the reports originating in this area. The second highest reporting department was the sales and marketing areas, representing 13% of reported incidents.

Employee Reported Spam, Virus, and Phishing

The shorter period and fewer number of observations in this data makes it difficult to draw strong inferences on the trend, although it follows a similar pattern as the privacy and security incidents.

When discussing employee incident reporting, the Information Security Officer described one January 2016 incident of an attempted business email compromise. An external threat forged the CEO's email address in a message to a YZ executive. The text of the email requested copies of W-2 tax information for all employees. The executive prepared a reply to the email but did not send it when the executive noticed the forgery in the return address. The executive notified the Information Security Officer, who followed up on the incident. Although no information was compromised, the Information Security Officer published a notice about phishing on the intranet and placed a large anti-phishing awareness poster outside the executive's office suite.

Headcount of YZ Organization

The headcount of YZ demonstrates a significant shift after the organizational changes made by the new CEO in 2015. According to the Head of IT, the corporate restructuring reduced the number of IT by more than half, eliminating the enterprise architecture and application development groups, with reduction in IT support across the board. The number and complexity of the business functions were not significantly reduced in this period, as the functions made obsolete by the 2010 regulatory change were already eliminated in 2012.

Headcount of YZ Information Security Team

The restructure split and reduced the information security team. The roles responsible for access management and administration of the network security devices moved to the IT infrastructure support group. The remaining team reported to the Information Security Officer and included two analysts for managing compliance, responding to alerts, and conducting risk assessments. For six months in 2015, the team consisted of a single analyst and the Information Security Officer, as team members departed after their colleagues had been laid off. The Head of IT mentioned that the security current staffing appears to be at its minimum, as "there may be problems in having enough people to have a separation of duties." The Head of IT added that some of the security functions are now being managed by cloud vendors and through consulting contracts.

Financial Performance of YZ Corporation

Although regulation stopped the primary input to YZ's revenue generating process in 2010, YZ continued to earn a steady revenue stream. The New Division did not contribute materially to the revenue during the period reviewed. In 2013, YZ's audited financials recorded a single "extraordinary expense" of $248 million. I removed this amount from the analysis numbers to better reflect the usual operating revenue and expenses of the organization. Although the revenue increased, YZ reduced expenses. The Head of IT remarked that IT felt the belt tighten as the CFO adjusted their performance metrics from on-time project completion to budget reduction.

The operating margin is an adjusted figure that removes non-performance related expenses and revenues from the calculation. The amounts used to adjust the margin may change from one year to the next. YZ's operating margin is a target set annually by management, and approved by the board, so it is a reliable figure of YZ's own target for financial success. YZ benchmarked the operating margin against like entities in 2015 and discovered the industry maintained an 8.86% operating margin. The Director of Internal Audit stated that, even after the adjustments, "many companies would kill to have YZ's operating margin."

From the trends in YZ's financial performance, the organization is reducing expenses, and increasing revenue. YZ is aware that the revenue from the legacy process will eventually decline. The financials do not yet reflect the investment and revenue in

the New Division. The perception in management of the potential instability of YZ's current state may not be reflected in what appears to be a healthy financial state.

Communications with the Board of Directors

From 2010 to 2014, only two board items addressed information security, the first to acquire funds to hire a consulting firm to perform a FISMA gap assessment, the second the report from consultants.

In the December 2015 meeting, a board member asked YZ's new head of internal audit to amend the internal audit plan to include a cybersecurity audit. In February 2016, the board held a discussion of enterprise risk management, which mentioned cybersecurity as a factor of enterprise risk. (My review of the board materials available did not find subsequent discussions of enterprise risk management.) At the same meeting, the CFO addressed information security in greater detail. The information security document included in the board materials was a list of nineteen items, thirteen that identified information security tools, the remaining six closely tied to FISMA control families. The presentation included a description of YZ's "commitment and investment in cyber security," and YZ's requirement for FISMA compliance as necessary to future federal contracting and as a Department mandate.

In February 2017, the agenda listed a discussion on IT strategy and cybersecurity, and included materials on YZ's approach, but discussion was postponed for the next meeting. The minutes from the May 2017 meeting describe the Head of IT's presentation. The Head of IT outlined a flexible strategy that relies on a "bias towards

cloud-based solutions" and reserving "costly custom build solutions for fundamental unique product offerings." "IT staff, the security team, outside resources, and security awareness" will be used to achieve its goals of "best practices through policies, standards, procedures, vendor management, business continuity, security, and compliance reviews, assessments and audits" according to the minutes. The minutes include a discussion of a "consolidated framework for cyber security strategy" that include a "single set of policies driving compliance needs."

The Head of IT described the board, and one member, as engaged in the discussion of security. That board member requested a standing board agenda item for information security. The board member asked the Head of IT if an incident like the 2006 breach could happen again. The Head of IT responded that it would not happen, due to the number of controls YZ implemented to prevent a vendor accessing protected data, especially non-public personal information.

Information security communications to the board appear to be evolving from a discussion of compliance activities, to preliminary discussions on information risk and effective means to manage multiple compliance approaches. The addition of a standing item on information security indicates that some members of the board view information security as part of their governance obligations. The routine meeting with the Head of IT establishes a line of communication and information sharing vertically from the board to the information security team.

The Cloud Strategy

In the February and May 2017 board materials, YZ's IT communicated its "bias to cloud based solutions" and reducing custom software "fundamental unique product offerings." The cloud bias began in 2015. Business areas, sensing a decrease in available IT resources, saw cloud options as an attractive alternative. IT viewed the cloud as a primary means to reduce cost and maintain service. Apart from a marketing and sales cloud product, YZ did not begin investing in cloud services until 2015. YZ began to implement a cloud-based security information and event management product in September 2015. According to the Information Security Officer, this implementation was designed to replace obsolete systems and reduce the workload on the reduced security staff. The vendor selected was unable to successfully implement a working system, and YZ ended the relationship in December 2016. According to the Information Security Officer, "selection of the vendor was a budget decision, but in the end there wasn't enough money." He added that "the vendor was new and made promises it couldn't back up." According to the Head of IT, YZ still plans to contract with a cloud SIEM vendor.

Prompted by the obsolescence of its data center back-up solution, YZ's IT began implementing cloud back-up storage for its legacy application in summer of 2017. In the fall of 2016, YZ explored the possibility of moving a sizeable portion of YZ's legacy system infrastructure to the primary hardware vendor's cloud service. Executive management evaluated the vendor's proposal and decided against the move due to the vendor's cost estimates. YZ's human resource group replaced their benefits, payroll, and

employee management systems to a cloud solution in January 2017, and the accounting department plans in 2018 to implement a cloud service to replace their on-premise system. IT implemented a cloud replacement for enterprise email and productivity software that also included a Cloud Access Security Broker (CASB) function. The CASB manages security controls to email and the productivity software. YZ plans to implement a cloud replacement for its financial system in May 2018. "The cloud is a mixed bag," the Head of IT stated, adding that it suits "commodity processes," but "line of business functions should stay here." The Head of IT also mentioned that "if you are required to use FEDRAMP for a cloud provider, we've found that it is usually cheaper to keep it on premise: it is saving us a lot of money."

The Information Security Officer and Head of IT both communicated the cloud strategy as a cost saving effort. They agreed that the case of the failed SIEM cloud implementation demonstrates that even as a cost saving, YZ should closely evaluate prospective cloud vendors. "In the end, all you have is a service level agreement that you hope they hold up," remarked the Head of IT.

Security Awareness Quiz

The error rate on the quiz responses provides an indicator of the signaling of information between the information security team and the employees in the rest of the corporation. According to the Information Security Officer, the information security team does not examine the results of the quiz.

As with the employee reported data, the percent of perfect scores on the quiz remains consistent despite the changes to the organization. YZ's corporate trainer, who manages the quiz software, commented in an interview on the limitations of the quiz. The software made changes to the questions difficult, and, in the trainer's opinion, has limited value as a learning tool. The trainer continues to use the software since it fits a specific compliance need not only for information security, but also other corporate compliance training. The trainer stated that other options were being explored, but the training resources had been significantly constrained since 2015.

DISCUSSION

What effect did YZ's FISMA catalogue of controls compliance program have on their security outcomes? Did the Department's decision to make FISMA controls mandatory, and the subsequent assessment, improve the level of YZ's security? In this section, I discuss the relationship between the investment in IT controls, and the results of the penetration test and compliance assessments. I will also examine how the information security department's interaction with changes in leadership and compliance requirements created a vertical emergent process toward the board of directors but did not develop a lateral process toward YZ's other business functions. Based on these results, I will discuss how a compliance-focused control catalogue implementation does not have a direct, reliable positive impact on security outcomes, and that organizations seeking to establish trust should explore alternatives that require a broader, organization-wide examination of risk. The results will be viewed through the perspective of information security at YZ Corporation, and information security when it operates within the intersection of multiple complex systems.

YZ accelerated its decrease in IT intensity in 2015 while implementing control catalogues for both the legacy and New Division systems. As illustrated in Figure 1, several measures hit their extreme points in 2016. IT intensity hits its lowest point, while penetration test findings peak and incidents rise. This confluence of events may have brought YZ's information security team to the "edge of chaos." The results for 2017 reverse direction, as emergent processes evolved within the reduced IT department.

Examination of the underlying data reveals a stronger relationship between the level of IT investment, the number of penetration test findings, and the qualitative results of the FISMA assessments and internal audit reports. The uncharacteristic increase in revenue for 2016 may exaggerate the acceleration of the IT intensity decline, but YZ management was unambiguous in its decision to reduce IT investment. YZ management created an IT performance measure based on the cost reduction of legacy support for 2015 through 2017. Research into security breaches at hospitals reported that investment in IT was not a reliable indicator of a hospital's level of security, but that other organizational culture factors may be more important (Angst et al, 2017). The study identified the integration of security within IT as more important than the investment, a process that occurred by necessity at YZ during the reorganization in 2015.

Due to the 2015 reductions in staff, the IT department had to support processes that were now missing key personnel. The increase in penetration test findings may indicate challenges in the vulnerability management program, which contributed to the results in the 2016 and 2017 FISMA assessments. The improvement in penetration test results in 2017 reflects the emergence of a process to address the vulnerabilities.

The privacy and security incident records reflect a different dynamic occurring in the organization. The number of incidents related to IT controls remained low, with only four reports in this category over five years. The number of email and lost device reports dropped significantly in 2015 when normalized for headcount. If the drop in the reports were the result of the implementation of a control, one would expect the decline to persist beyond 2015, but the incident reports rose in 2016, and remained above 2015 levels in

2017. The incident reports rely on employees to report an event that management may perceive as a performance deficiency. An employee may be more reluctant to self report during a period of organizational instability.

The security quiz scores remained stable throughout this period, with roughly the same percentage of the organization overall achieving perfect scores from 2013 to 2017. This score persisted despite the changes to the organization and the shifting focus of IT. The quiz results may reflect properties of the quiz format more reliably than as a metric of how employees would act to protect data. The primary function of the quiz is the implementation of a security control, so stability in the quiz scores should correlate with incident reporting. The stability of the quiz scores when compared with the variation in the incident reporting may illustrate a lack of linkage between mandated compliance controls and security outcomes.

Based on the comments of the Information Security Officer, the relationship between information security and the rest of the organization was never close. The internal audit findings regarding the difficulties in assessing risks and implementing cloud services demonstrate a breakdown in communications between the information security team and operational areas. The information security team did not administer or review the results of the awareness quiz, delegating the task to the human resources department. The information security team may not have focused on the quiz or the incident reporting processes, since they were in a stable, compliant state. Despite the participation of human resources and building management in security activities, the Information Security Officer commented that the corporation at large viewed “security as

IT's job," a comment that he followed up with the observation that IT and other departments "never got along well." Parsons' research on information security culture reflects a complex relationship between awareness activities, policy compliance, and employee behavior (Parsons et al., 2015). Bauman describes the tension between organizational units as a feature of complex adaptive systems, calling the "concurrency of multiple, and often conflicting, performance measures and reward structures, which define the goals that decision makers attend to" a "central characteristic of real organizations" (Baumann, 2015). A new emergent process of awareness and incident reporting between information security and the rest of the organization does not appear to have evolved.

Although the information processing did not occur laterally across the organization, an emergent process evolved vertically as information sharing began between the information security team and the board of directors. The interest in information security by a single board member both generated activities by the internal audit team and established regular communication with the information security team. The comments by the Head of IT reflected that the board member's interest was focused more on reducing the risk of a breach than with compliance and control catalogue implementation.

The challenges of supporting an end-of-life legacy system are illustrated in both the penetration test findings and the FISMA assessment. During this period, YZ made few changes to the web application that supports YZ's legacy business operations. The information security team tried to balance the business needs of system stability and cost

reduction against the security and control catalogue requirement to patch vulnerabilities in the web application's core middleware components. The "cloud bias" strategy is unlikely to reduce the effort required by YZ to maintain the web application evaluated by the penetration test, but the Head of IT's assertion that "the line of business should stay on-premise" would indicate that the web application will remain the responsibility of YZ. The web application is also intertwined with the legacy client server and mainframe systems, and it supports a business function that will become obsolete in five to ten years. Recent research (Pang and Tanriverdi, 2017) showed that moving legacy systems to the cloud can reduce information security risk in federal systems. For YZ to commit to a cloud investment for its legacy web application, the information security risk would need to outweigh the risk of moving a complex, end-of-lifecycle system to a FEDRAMP compliant environment. YZ's IT team may have difficulty in making this case for cloud migration to business owners that demand stability.

The FISMA assessments are targeted directly at the legacy system and the control catalogue implementation but provide ambiguous results. A reader of the two FISMA assessments could infer a decline in outcomes from 2016 to 2017. The 2017 report reported an almost hundredfold increase in itemized risks over the 2016 report. Five of the eight 2017 POAM items carried over from 2016, which may reflect a decreased ability to remediate control weaknesses. Combined with information on the loss of budget and staff for the IT and security processes, a reader could assume from the 2017 assessment's executive summary that YZ's FISMA program was struggling, a conclusion opposed to the results of the penetration tests, which indicate a recovery from 2016

results. YZ's IT and security teams objected to the assessment team regarding the content and format of the 2017 report.

The 2017 assessment report combined the presentation of vulnerabilities, risks, and controls. The assessment made no distinction between a risk and a vulnerability in its executive summary, and the YZ team felt that a reader would not be able to make the distinction between a control weakness and single instance of unpatched software. The security team felt the assessor's use of YZ's own vulnerability scan was "throwing our own scans back at us." The scan included many systems that were not in FISMA scope. YZ IT management felt the assessor's report, based on this information, did not accurately communicate YZ's risks, or YZ's compliance with the control catalogue. The scan results mapped to a single control (RA-5) of the 262 controls assessed in 2016, and of the 143 assessed in 2017. The assessors' report did not account for the functions of the systems, the assets they stored, or the compensating controls YZ had implemented. YZ's Information Security Officer expressed concern about the results being misinterpreted by two types of assessment readers. The first type of reader was the Department, an external entity that had significant power over YZ. The second type of reader was YZ's leadership and board of directors, who could view the report as an indicator of YZ security program's deficient performance.

The Head of IT and Information Security Officer's objection is fundamental to the nature of the control catalogue used as a compliance measurement. Measurement against a compliance framework is designed to provide assurance that the "organization has designed and implemented appropriate controls to mitigate cyber risks"

(Galligan, 2015). The framework also provides a path to establish trust with third parties. In YZ's instance, approval by the Department was the primary driver for their move from using the control catalogue as a set of best practices to using the control catalogue as a mandatory compliance activity. The information security team felt the assessment report was not an accurate reflection of the design and implementation of their controls, and that the assessment would not provide the Department with sufficient information to evaluate YZ's security program. The reliability of assessments to perform trust decisions is not unique to YZ's situation. Investors question the reliability of financial statements after the collapse of firms with audited financials. Kaplan argued that "shareholders cannot assess the quality of an audit report even after its been consumed" (Kaplan, 2007). Equifax's assessors reported compliant states across a number of control catalogues, and yet they suffered a catastrophic data breach. Although YZ's assessors did not make a judgment on YZ's compliance, the results illustrate the possibility that an ambiguous assessment may not allow a trustworthy organization to be trusted.

YZ's IT department identified the maintenance of the legacy web application as a cause for the numerous risks identified by the FISMA assessors. The compensating controls YZ had deployed to protect the web application appeared to be working as intended based on the penetration test reports. The FISMA reports did not reflect this condition. According to the 2017 internal audit memorandum, YZ's own internal audit department performed significant analysis and verified information with the security team before it was able to conclude on the information security risk associated with the results of the 2017 FISMA assessment.

Freund and Jones mention that they "have yet to see (or even imagine there being) an organization that is 100% compliant across its entire risk landscape" (Freund and Jones, 2015). YZ's concern that the FISMA assessment would not accurately reflect their controls implementation may not be unique or unfounded. In their examination of FTC expectations of "reasonable security," Breaux and Brummer state that technical standards help organizations plan, and "can provide technical guidance that can be used to strategize how to comply with security laws" The approach of "reasonable security" is to "thwart attacks and prevent or diminish violations of security laws" (Breaux & Baumer, 2011). YZ had used the FISMA standards and control catalogue in this fashion since 2010, and the Head of IT confirmed that they "improved security." YZ's information security team did not, however, have experience in managing compliance and assessments. Lance Hayden described information security compliance culture as a culture where "the cardinal directive can be expressed as *pass audits*." He adds that "while 'good security' almost always equates to good compliance, becoming a matter of translating a security program into the language of whichever auditor is reviewing it, good compliance does not necessarily equal good security" (Hayden, 2016). As demonstrated by YZ, the method of translating "good security" to "good compliance" may not be an effortless process, and it poses a riskier task for smaller organizations with constrained resources. The system of control catalogues and assessments also demand a level of systemic thinking that is counter-productive in a complex system and "may well increase the disorder" according to Ralph Stacey (Stacey, 1996).

A very pragmatic, tactical recommendation to YZ and other organizations faced with information security compliance obligation and limited resources would be to focus on the management of the assessment and restrict the flow of information to the assessors. This approach would reallocate resources away from effective security controls yet would increase the probability of a certification. As illustrated by the Equifax example, this process would not yield long term business success or maintain trust with customer and business partners.

A longer-term solution should take a broader approach to security compliance certification beyond the creation of a checklist of controls. A security framework that examines an organization's assets, evaluates its industry's threats, and prioritizes control implementation could provide third parties a trustworthy certification. This approach would cost more, take longer, and place an unreasonable burden on smaller organizations. Another potential method would reduce significantly the number of controls required for compliance, but the controls could be selected based on the assessed organization's business sector.

This research centered on a case study of a single organization, so there may be limits on the applicability of the results to other organizations, or to an effective system of regulation. YZ Corporation experienced several significant changes in governance, personnel, and strategy during the period studied. YZ also had an uncommon business model, serving a federal government function as a non-profit organization. This business model provides an environment without the influence of traditional stakeholders associated with public or private for-profit companies. Also, YZ did not maintain a set of

information security metrics, which would have provided additional data to track security outcomes and measure the impact of the compliance effort. The results do provide an illustration of the dynamics of a complex system, and how regulation of control catalogues highlight the tension between the goals of trust and the goals of information security.

Additional research into the impact of control catalogues on security outcomes could offer additional insight into the phenomena. A broader review of different business models and stakeholders, and how they approach information security compliance, could identify additional models for the dynamics between trust and information security. Research into how organizations establish trust, and how reliant they are on third-party information security assessments in establishing their trust, could assist organizations in determining the level of investment into the assessments.

CONCLUSION

Control catalogues as required by regulation may not have management's desired impact on the security outcomes of an organization. Regulations with control catalogues persist because of their efficiency in providing certification used to establish trust between organizations. Measuring an organization based on its ability to implement a selection of best practices may not produce consistent or even representative indicators of the organization's security outcomes.

Potential remedies to the problem might include replacing the control catalogues with systems that would require the information security team to gather more information directly from the business functions and employees. An alternate method of presenting this information could lay a better foundation for informed trust between information trading partners, while fully supporting the information security goals.

This research has begun to address the gap in the literature that addresses the larger issue of the relationship between security compliance and security outcomes. Ideally these objectives of compliance and security should be aligned, but the structure of compliance as a control catalogue may not be the optimal design to achieve this goal. A regulatory framework should establish trust based on the ability of an organization to reduce information security risk, and innovative approaches should be considered.

BIBLIOGRAPHY

AICPA. (2017). *Reporting on an Entity's Cybersecurity Risk Management Program and Controls 2017*. John Wiley & Sons, Inc.

Anderson, P. (1999). Complexity Theory and Organization Science. *Organization Science*, *10*(3), 216–232.

Anderson, R. (2001). Why information security is hard: An economic perspective. In *Computer security applications conference, 2001. acsac 2001. proceedings 17th annual* (pp. 358-365). IEEE.

Angst, C. M., Block, E. S., D'arcy, J., & Kelley, K. (2017). When do IT security investments matter? Accounting for the influence of institutional factors in the context of healthcare data breaches. *MIS Quarterly, 41(3)*, 893-916.

Baumann, O. (2015). Models of complex adaptive systems in strategy and organization research. *Mind & Society*, *14*(2), 169–183.

Breaux, T. D., & Baumer, D. L. (2011). Legally "reasonable" security requirements: A 10-year FTC retrospective. *Computers & Security*, *30*(4), 178–193.

Burnes, B. (2005) Complexity theories and organizational change. *International Journal of Management Reviews*, 7(2), 73-90.

Burns, A. J., Posey, C., Courtney, J. F., Roberts, T. L., & Nanayakkara, P. (2017). Organizational information security as a complex adaptive system: insights from three agent-based models. *Information Systems Frontiers*, *19*(3), 509–524.

Cheney, J. (2010). *Heartland Payment Systems: Lessons Learned from a Data Breach*. FRB of Philadelphia - Payment Cards Center Discussion Paper No. 10-1. Available at SSRN: https://ssrn.com/abstract=1540143

Coffman, D., Agrawal, B., & Schaffa, F. (2013). Towards Optimal Risk-Aware Security Compliance of a Large IT System. In *Service-Oriented Computing* (pp. 639–651). Springer, Berlin, Heidelberg.

$(ISC)^2$. (n.d.). *Compliance Mapping Certificate*. Retrieved July 27, 2017, from https://www.isc2.org:443/Training/Compliance-Mapping-Cert-Program

Edwards, B., Hofmeyr, S., & Forrest, S. (2016). Hype and Heavy Tails: A Closer Look at Data Breaches. *Journal of Cybersecurity*, *2*(1), 3–14.

Equifax. (2017a, September 15). *Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes* [Press release] Retrieved from https://investor.equifax.com/news-and-events/news/2017/09-15-2017-224018832

Equifax. (2017b, November 9). *Equifax Releases Third Quarter Results* [Press release] Retrieved from https://investor.equifax.com/news-and-events/news/2017/11-09-2017-211550295

Freund, J., Jones, J. (2015) *Measuring and Managing Information Risk: A FAIR Approach*. Elsevier

Galligan, M. E., & Rau, K. (2015). *COSO in the Cyber Age*. Deloitte, January.

Gordon, L. A., & Loeb, M. P. (2002). The Economics of Information Security Investment. *ACM Trans. Inf. Syst. Secur.*, *5*(4), 438–457.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015). Increasing cybersecurity investments in private sector firms. *Journal of Cybersecurity*, *1*(1), 3–17.

Grobman, G. M. (2005). Complexity Theory: A new way to look at organizational change. *Public Administration Quarterly*, *29*(3/4), 350–382.

Hayden, L. (2009) Designing Common Control Frameworks: A Model for Evaluating Information Technology Governance, Risk, and Compliance Control Rationalization Strategies. *Information Security Journal 18*, 297-305.

Hayden, L. (2016). *People-Centric Security*. McGraw-Hill Education.

HITRUST. (2017). *HITRUST CSF Version 8.1*. HITRUST.

Hubbard, D. (2009). *The Failure of Risk Management: Why It's Broken and How to Fix It*. John Wiley & Sons, Inc.

International Organization for Standardization. (2013). *Information technology - Security techniques - Code of practice for information security controls 27002:2013*. ISO/IEC.

Julisch, K. (2008). Security Compliance: The Next Frontier in Security Research. In *Proceedings of the 2008 New Security Paradigms Workshop* (pp. 71–74). New York, NY, USA: ACM.

Julisch, K., Suter, C., Woitalla, T., & Zimmermann, O. (2011). Compliance by design – Bridging the chasm between auditors and IT architects. *Computers & Security*, *30*(6), 410–426.

Kaplan, S., Roush, P., Thorne, L. (2007) Andersen and the Market for Lemons in Audit Reports. *Journal of Business Ethics*, 70(4), 363-373

Leszcz, M. (2017). *Trust Frameworks for Identity Systems*. Retrieved from http://www.openidentityexchange.org/blog/2017/06/22/trust-frameworks-for-identity-systems/

Lipner, S. (2015). The Birth and Death of the Orange Book. *IEEE Annals of the History of Computing* (37)2, 19-31.

Lipner, S., Lampson, B., (2016) *Risk Management and the Cybersecurity of the U.S. Government: Input to the Commission on Enhancing National Cybersecurity* retrieved from https://www.nist.gov/sites/default/files/documents/2016/09/16/s.lipner-b.lampson_rfi_response.pdf

Liu, Y., Sarabi, A., Zhang, J., Naghizadeh, P., Karir, M., Bailey, M., & Liu, M. (2015). Cloudy with a Chance of Breach: Forecasting Cyber Security Incidents. In *Proceedings of the 24th USENIX Conference on Security Symposium* (pp. 1009–1024). Berkeley, CA, USA: USENIX Association.

Mitchell, M., (2009). *Complexity: A Guided Tour*. Oxford University Press
Mock, T. J., Sun, L., Srivastava, R. P., & Vasarhelyi, M. (2009). An evidential reasoning approach to Sarbanes-Oxley mandated internal control risk assessment. *International Journal of Accounting Information Systems*, 10(2), 65–78.

OWASP. (n.d.) *OWASP Top Ten Project - OWASP.* Retrieved November 5, 2017, from https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

Pang, Min-Seok and Tanriverdi, Hüseyin. (2017). Security Breaches in the U.S. Federal Government (March 7, 2017). Fox School of Business Research Paper No. 17-017. Available at
SSRN: https://ssrn.com/abstract=2933577 or http://dx.doi.org/10.2139/ssrn.2933577

Parsons, K M., Young, E., Butavicius, M. A., McCormac, A., Pattinson, M. R., & Jerram, C. (2015) The influence of organizational information security culture on information security decision making, *Journal of Cognitive Engineering and Decision Making, 9*(2), 117-129

PCI Security Council. (2016, April) *Payment Card Industry Data Security Standard: Requirements and Security Assessment Procedures v 3.2.* PCI Security Standards Council, LLC.

Phister, J. (2010). *Cyberspace: The Ultimate Complex Adaptive System*. Air Force Research Lab, Rome, NY. Retrieved from http://www.dtic.mil/docs/citations/ADA540684

Ponemon Institute. (2017) *Ponemon Institute's 2017 Cost of Data Breach Study: Global Overview.* Retrieved November 2, 2017, from https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN&

Power, M. (2009). The risk management of nothing. *Accounting, Organizations and Society*, *34*(6), 849–855.

Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity*, *2*(2), 121–135. https://doi.org/10.1093/cybsec/tyw001

Ross, R. S. (2013). *Recommended Security Controls for Federal Information Systems and Organizations* [includes updates through 9/14/2009]. Special Publication (NIST SP) 800-53 Rev.4).

Sollis, D. (2010). Compliance for Compliance's Sake? *ISACA Journal* (2010) retrieved from https://www.isaca.org/Journal/archives/2010/Volume-1/Pages/Compliance-for-Compliance-s-Sake-1.aspx

Stacey, R. (1996). *Complexity and Creativity in Organizations*. Berrett Koehler.

Van Oosten, C., Hackett, S., Turner, A. (2017) *Verizon 2017 Payment Security Report*, Verizon

Weiss, N. E., & Miller, R. S. (2015). The target and other financial data breaches: Frequently asked questions. In *Congressional Research Service, Prepared for Members and Committees of Congress February* (Vol. 4, p. 2015).