Title: Information Security as a Competitive Advantage
Course: Strategic Management of Technology (ETM-526)
Year: 2015
Author(s): Claudiu Rusnac
Report No.: 6

Abstract:

This paper outlines how information security can be used as a competitive advantage and how information security fits into traditional business strategic models. The paper will also outline what components of an information security program are necessary to be incorporated into an organization’s business strategy that can be used as a competitive advantage.

Information Security as a Competitive Advantage

Claudiu Rusnac

Strategic Management of Technology (ETM-526)

Dr. Charles Weber, Spring 2015

1 Abstract

This paper outlines how information security can be used as a competitive advantage and how information security fits into traditional business strategic models. The paper will also outline what components of an information security program are necessary to be incorporated into an organization's business strategy that can be used as a competitive advantage.

2 Introduction

In a recent survey (2013) done by the United Postal Service identified that seventy percent of online shoppers prefer to conduct transactions to their favorite retailer via the Internet. [1] Other research done by Forrester Research also points to the fact that the American consumer spent more than $200 billon online and is expected to grow to a staggering $327 billion by 2016. [2] As organizations continue to expand their online presence, providing a secure method of doing business becomes imperative to the success of an organization. Information security is becoming a differentiator and can be viewed as a competitive advantage. The role of securing customer data, intellectual property, and providing secure methods to conducting business over the public Internet becomes a core component of a business strategy.

TD Ameritrade CEO Fred Tomczyk, was asked in a televised interview about what "keeps him up at night?" Tomczyk replied that a major concern regarding his organization, and the overall economy, was cyber security. [3] Similarly, in a 2015 Protiviti survey of 277 top-level executives across various industries, identified that 53 percent of organizations are not prepared to manage cyber risk that will significantly impact their organizations'. [4] As the market economy continues forward to an Internet

based economy and less dependent on a traditional brick-and-mortar infrastructure, information security needs to be part of an organization's business strategy.

This paper will outline how information security can be used as a competitive advantage and how information security fits into traditional business strategic models. The paper will also outline what components of an information security program are necessary to be incorporated into the business strategy that can be used as a competitive advantage.

3 The Growing Cyber Threat

Cyber threats are on the rise and attackers are becoming more and more sophisticated on how they exploit weaknesses or vulnerabilities within an organization. Security organizations, such as, Symantec identified that there was a 23 percent increase in data breaches in 2013. The external threat is becoming significantly more sophisticated and organizations are having a hard time adapting to the growing threat. "As organizations look to discover attackers using stolen employee credentials and identify signs of suspicious behavior throughout their networks, savvy attackers are using increased levels of deception and, in some cases, hijacking companies' own infrastructure and turning it against them." [5] The charts below (Figure 1, Figure 2) outline the growing number of breaches that are occurring over the entire spectrum of organizations and industries. The table below highlights some of the largest data breaches across industries that have occurred within the last couple of years.

Company	Year	Customers Affected	Details
Anthem [6]	Feb 2015	80 M	Hacker accessed names, birthday, member IDs, SSNs, and other personal identifiable information.
Home Depot [7]	April / May 2014	56 M	Russian Hacker group stole credit card data from ~2200 stores.
JP Morgan Chase [8]	July 2014	76 M	Hackers stole names, addresses, phone numbers, and emails of account holders.
Target [9]	Nov / Dec 2014	70 M	Hackers were able to steal customer information via malicious hardware installed on magnetic strip readers in Target stores.

The above research/data makes an overwhelming case: each type of organization, whether delivering goods or services over the Internet, or providing services such as healthcare, are susceptible to attacks and need to consider information security as part of their strategic objectives. Simply put, it is not a matter of *if*, it is a matter of *when* an organization will sustain a targeted attack. Organizations that incorporate a mature information security program as a component of their business objectives, will be better positioned to prevent, deter, or minimize the impact of the information security breach; allowing the organization to use information security as a competitive advantage.

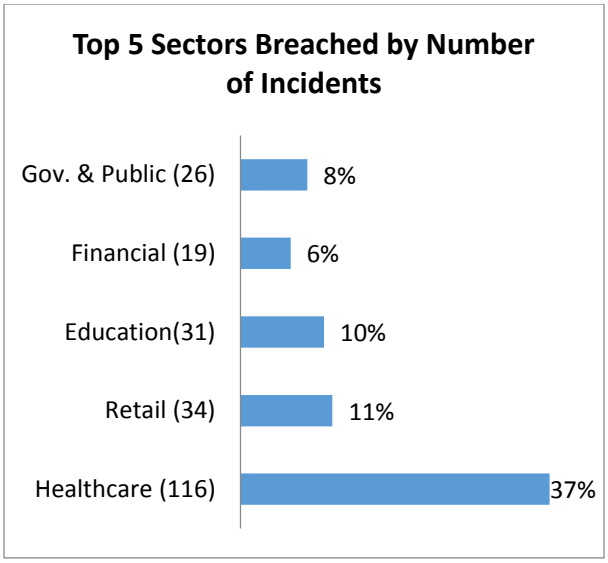

Figure 1 - Top 5 Sectors Breached by Number of Incidents, Symantec 2015

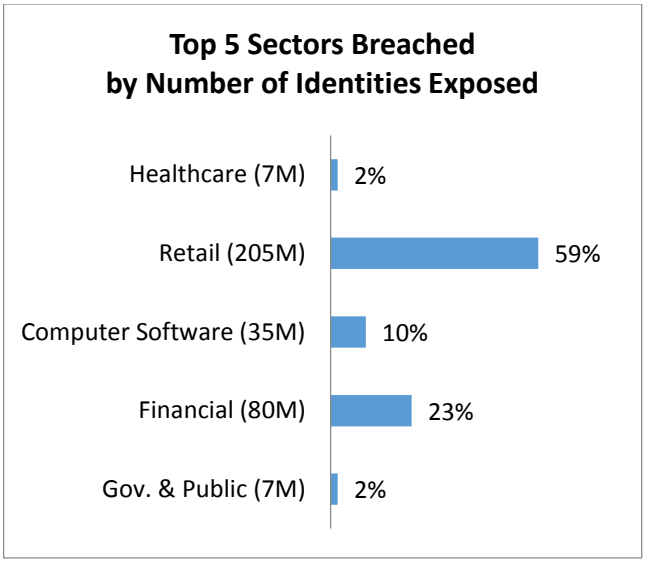

Figure 2 - Top 5 Sectors Breached by Number of Identities Exposed, Symantec 2015

4 Defining Information Security

Information security has traditionally been viewed as cost overhead - similar to an insurance policy. It is only useful when you need it – usually after a large incident. Efficiency, products features, and business growth models have always taken precedent over securing an organization's network and data. The task of protecting information (customer information, intellectual property, etc.) is generally a function of the Information Technology (IT) department, but as recent disclosures of large data breaches show, the task of information security is becoming a core component of the overall business strategy and is a responsibility of the organization as a whole.

Information security has many facets, but one can define information security in the context of the Confidentiality, Integrity, and Availability (CIA) Triad model. The CIA triad (Figure 3) is used to evaluate the information security posture of an organization, or even an independent system at a granular level. The primary goal of the CIA triad

provides a standard methodology of evaluating information security controls irrespective of the platform and technology used to develop a business system. [10] In the context of this paper, the CIA triad will be referenced as a necessary holistic framework required for an information security program to be viewed as a competitive advantage. A mature information security program that can be viewed as a competitive advantage needs to include and demonstrate all aspects of the information security CIA triad model. The following sections below further define the CIA triad model.

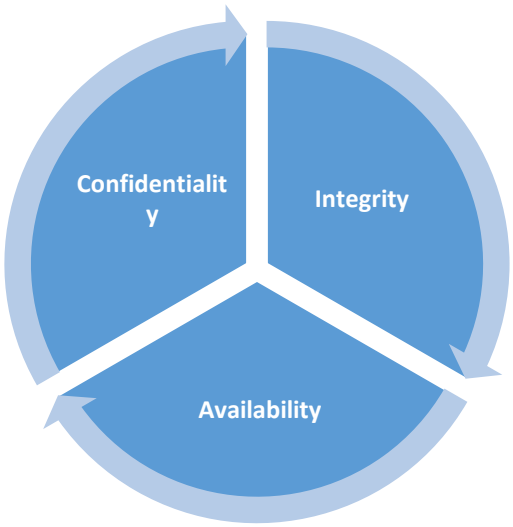

Figure 3 - CIA Triad Model

4.1 Confidentiality

In a broader concept, confidentiality can be referred to as data privacy. All information requires a specific classification and according to that classification, data needs to transmitted or stored with the necessary protections in place. For example, when transmitting a credit card via the Internet, properly implemented security controls would dictate, that end-to-end (from the end-user's computer to the server that processes the credit card) communication be encrypted. This protection provides the

confidentiality required to prevent identity theft and other risks associated with improperly securing data.

4.2 Integrity

Integrity refers to information reliability and the assurance that data has not been tampered with. As information is transmitted or stored it is necessary to have the confidence that information has not been tampered with. For example, it is necessary for software applications to properly validate transaction data for the correct values when processing or storing the information. By properly validating data, one can confidently ensure that data has not been tampered with during transport. A sub-component of integrity is non-repudiation. Non-repudiation is the automated function that logs who, what, and when a resources has been changed or accessed on an IT system. Non-repudiation prevents forgery and tampering of data. Non-repudiation is also used to prove that an authorized user intended to alter or send data within an IT system.

4.3 Availability

Availability refers to IT resources being accessible to serve its respective purpose. IT computing resources are required to be accessible when internal or external parties interact with critical IT assets. For example, it is critical that large e-commerce websites maintain load-balanced systems to prevent a denial-of-service attack. The denial-of-service attack would restrict or impair the business from selling goods or services via its online portal. Other aspects of availability include backup, business resumption, and redundant systems.

The table below summarizes some of the associated risks and controls that one must consider in the context of the CIA triad model. [11] Similarly, a mature information security program will incorporate controls that include all aspects of the CIA triad.

CIA	Risk	Controls
Confidentiality	• Loss of privacy • Unauthorized access to information • Identify Theft	• Encryption • Proper authentication, authorization and access controls
Integrity	• Information is no longer reliable or tampered with in the process of transmission in a undetectable manner	• Integrity Checking • Proper Quality assurance methodologies • Audit logging • Digital signatures
Availability	• Disruption to business or denial of service • Loss of customer confidence • Loss of Revenue	• Proper business continuity • Risk Assessment Process • Backup / restoration processes

Table 1 - CIA Risk and Controls

4.4 Capability Maturity Model

It is simply not sufficient enough to implement an information security program, but rather it is necessary for the information security program to be mature in its processes to be considered a competitive advantage. The Capability Maturity Model (CMM) can be used to evaluate a program within the context of the CIA triad. The CMM model has five maturity levels (see table below), which can be used to evaluate an information security program. In the context of this paper, it is necessary that an information security program be a minimal CMM level 4 to be considered a competitive advantage. By definition, a CMM level 4 processes within an information security program has predictable and uses quantitative methods to control processes. By using quantitative measurements, the information security program is adaptable according to

the changing threat landscape and predicts the program's effectiveness. [12] Furthermore, processes at CMM level 4 are adaptable, which give the information security program the ability leverage existing processes to other aspects of the business to identify emerging threats.

CCM Level	Definition
1 Initial	The initial process does not have structure, undocumented, uncontrolled and general a reactivate set of ad-hoc events.
2 Repeatable	Processes at this level are generally repeatable and in some cases produce consistent results.
3 Defined	Processes at this level are established and documented. The process will also improve over time.
4 Managed	Processes at this level are measurable using quantitative metrics. The processes in level 4 can be adjusted without measurable los of quality or deviation from specifications.
5 Optimizing	Processes at this level are focusing on improving process performance.

Table 2 - Capability Maturity Model (CMM) [12]

4.5 Competitive Advantage as defined by Business Models

The textbook definition of competitive advantage is "a superiority gained by an organization when it can provide the same value as its competitors but at a lower price, or can charge higher prices by providing greater value through differentiation. Competitive advantage results from matching core competencies to the opportunities." [13] Michael Porter further defines two types of competitive advantages: differentiation and cost advantage. Cost advantage exists when an organization is able to deliver same goods or services at a lower cost compared to its competitors. Differentiation is when an organization can provide additional benefits that exceed its competition. [14] Other models such as the resource-based view define competitive advantage in relation to the organizations resources and capabilities. These superior resources and

capabilities result in additional value creation that exceeds the organization's competition.

Each competitive advantage model has limitations, and does not sufficiently encompass information security, so it is necessary to integrate both models (porter and the resources-based view) to describe how information security fits in as a competitive advantage. [15] The figure below combines both models and highlights that resources, capabilities, combined with cost advantage or differentiation is what ultimately will create the value and inherently a competitive advantage.

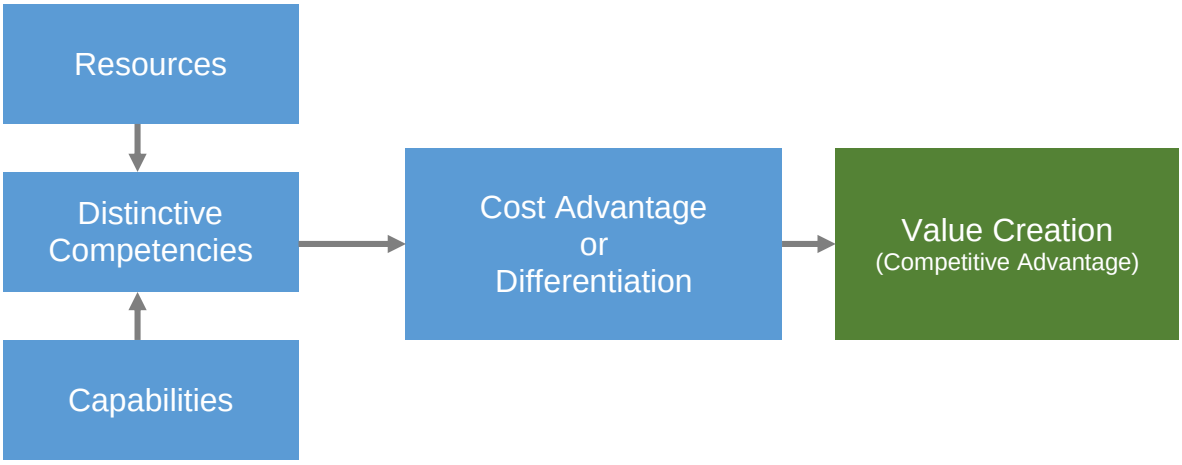

Figure 4 - Combined Competitive Advantage Model [15]

In the context of this paper, it is important to identify what resources, competencies, and capabilities, which can be used as differentiation and ultimately be used as an organization's competitive advantage. The following sections outline aspects of an information security program that an organization should consider implementing and the will ultimately provide competitive advantage. In order for information security to be considered a competitive advantage, the following aspects of an information security program need to be implemented in a CMM level-4.

4.6 Information Security Program as a Competitive Advantage

The following sections outline core components of a mature information security program that should be implemented in order to be considered a competitive advantage. Furthermore, the components of the information security program should be operating at a minimal CMM level-4.

4.6.1 Information Security Know-How

As stated in previous sections, the cyber security threat is continuous and the threat landscape is constantly changing. To that end, it is necessary that an organization have properly trained information security staff to develop processes, tools, and policies to deal with current and future threats. Without properly trained information security staff, threat information cannot be translated to actionable tasks to secure an organization's networks and data. Forrester outlines two main components that must be considered when building and training an information security team [16]:

- **Diversity strengthens the team** – The more diverse team, the better. Information security staff with cultural/geopolitical knowledge, business unit knowledge, language skills, intrusion detection, incident handling, penetration testing, scripting, and programming experience all deliver value and provide a unique perspective.
- **Look for the intangibles** – An analytical mind and critical thinking skills are the foundation for any good information security professional. Highly skilled information security professionals are able to draw conclusions from disparate data points and make rapid decisions in the context of a changing threat landscape.

4.6.2 Enterprise Risk Assessment

Protiviti, a independent consulting organization, defines Enterprise Risk Assessment (ERA) as “a process, effected by an entity’s board of directors, management and other personnel, applied in strategy-setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.” [17] The over-arching goal of ERA is to identify, evaluate, mitigate, and monitor risks within the context of the organization’s business objectives. In many cases, risk is cannot be removed all together, but rather reduced to an acceptable level. In order to reduce risk to an acceptable level throughout the organization, using a general ERA process of Identify, Evaluate, Mitigate, and Monitor (IEMM) for risk is used. The following sections below further define IEMM.

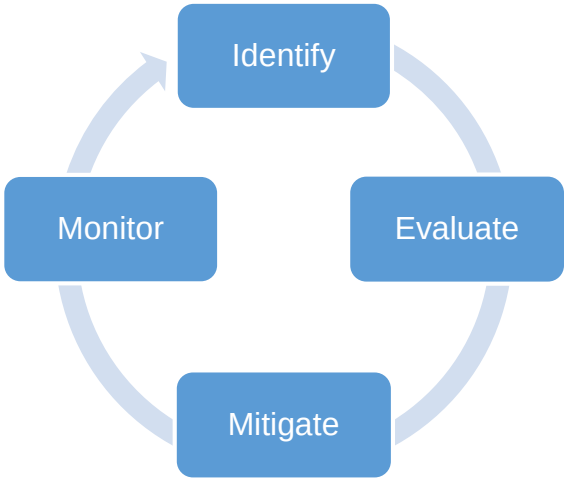

Figure 5 - Enterprise Risk Assessment Process

Identify Risks

Identifying risks is the first step to an ERA process. This step will dictate the necessary investments, priorities and opportunities that the information security

program needs to focus on. Risks can be identified, by using automated tool such as vulnerability scanners, network intrusion prevention systems, firewalls, log correlation engines, and many other various security automation technologies. System and network architectural reviews and performing scenario testing is also required to identify systemic weaknesses in IT systems.

Evaluate Risks

Once a risk has been identified, the risk(s) needs to be evaluated in the context of security controls to determine, if any, necessary actions are required. In order to evaluate a risk, the risk formula [18] can be used to determine if a risk requires any action.

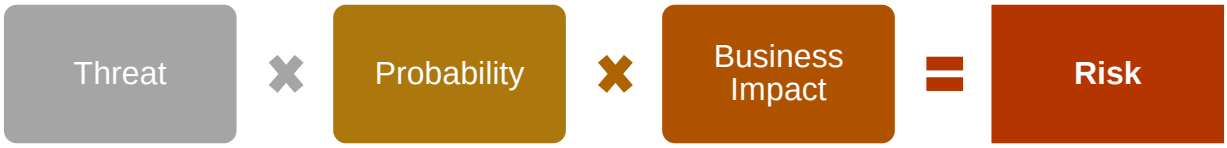

Figure 6 - Threat Formula [18]

By using the threat formula, each risk can be independently evaluated which will determine if the risk can be accepted, mitigated or reduced, or in some cases transferred to a third party (insurance).

Mitigate Risks

The goal of the mitigate risk(s) step is to implement security controls that will lower the probability of a security event occurring and by lowering the impact of the identified risk when it does occur. By minimizing or potentially removing a risk from the organization's environment, the organization will be able to operate with minimal disruptions.

Monitor Security Controls and Emerging Threats

Once security controls have been implemented, it is necessary to monitor their effectiveness in the context of continual and emerging threats.

4.6.3 Employee Information Security Training & Security Policy

In many cases, information security threats are not sophisticated, but rather prey on untrained employees who are unaware that they are being targeted. Social engineering attacks such as, malware infected sites, phishing emails, etc., entice the user to divulge sensitive information. These threats lead to infecting a users system with viruses, Trojans, and other malware that ultimately pose a serious threat to an organization's internal IT infrastructure. It is necessary that organizations develop a security policy and train users how to identify threats and how to deal with various threats when they become compromised.

4.6.4 Defense-In-Depth

No single information security solution is sufficient enough to provide the necessary protection of IT assets within an organization. To that end, it is necessary to employ a defense-in-depth approach to information security and risk management. By doing so, an organization should layer its security defenses and employ multiple technologies and processes to holistically decrease the organization's risk. The basic defense-in-depth principle is that, with each layer of protection, certain controls are in place and if a security control (defense) fails, the other layers mitigate the risk to an acceptable level. See figure below.

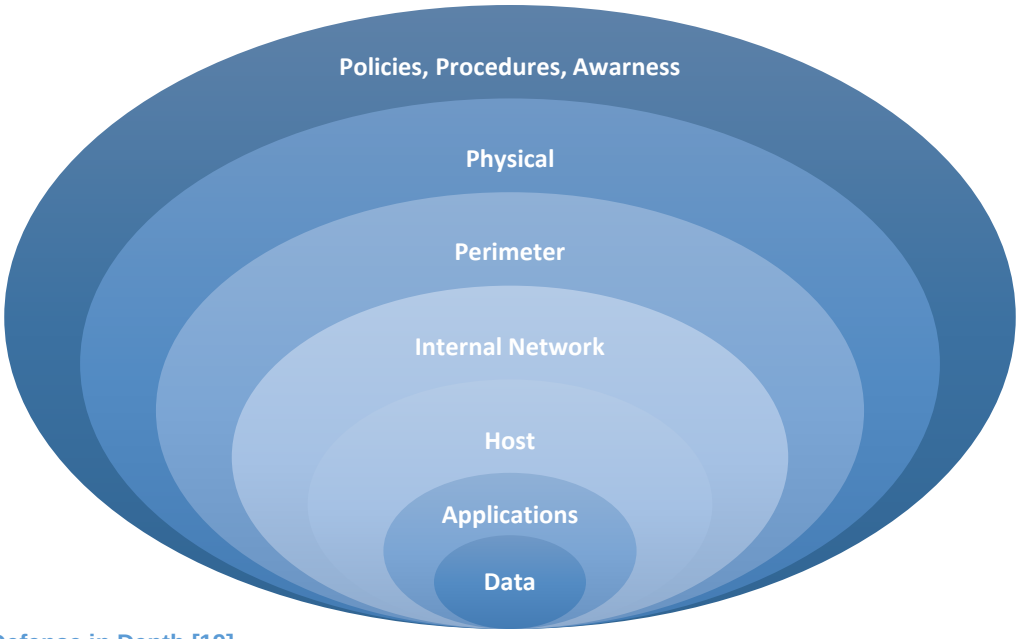

Figure 7 - Defense in Depth [19]

5 Challenges to Implementing a Information Security Program

This paper has outlined the necessary components of an information security program that need to be implemented and effectively managed to provide an organization with a competitive advantage. From a theoretical perspective, the proposed information security program, as defined above, provides a framework for implementation. But in the real world, information security programs have significant implementation constraints. The SANS Institute, a industry pioneer in information security training and research outlines some of these constraints: [20]

- Business realities and financial obligations determine what is a business priority thus limiting investment in the information security program.
- Existing IT investments, in many cases, do not allow organizations to change rapidly to existing or emerging threats.
- Legal and regulatory requirements often dictate where resources are expended and generally are not effective in dealing with emerging threats.

Even though real-world application of the defined framework does have implementation constraints, organizations need to invest and prioritize resources in a mature information security program. By doing so, organizations will not only better position themselves (differentiation) against their competition, but also create a competitive advantage for the organization.

6 Conclusion and Future Research

This paper has outlined how information security can be used as a competitive advantage from both a business model perspective and also from an information security practitioner's perspective. This paper also outlines a general framework that can be used to implement an information security program and provides a starting point for future research. Future research can include the following:

- Expand the competitive advantage concepts with other business models. Do certain business models comprehend information security better than others?
- Use the models described above as a starting point to compare organizations that have implemented a mature information security program and how they compare to their competitors.
- Expand other aspects of a information security program.

7 References

[1] B. Morris, “More Consumers Prefer Online Shopping,” *Wall Street Journal*, 03-Jun-2013.

[2] W. STU, “Online-Retail Spending at $200 Billion Annually and Growing,” *Wall Street Journal*, p. 1, 27-Feb-2012.

[3] “TD Ameritrade CEO Tomczyk: ‘Not Obvious We’ve Hit Bottom’ on Oil Prices,” *Think Advisor*, 29-Jan-2015.

[4] “Cybersecurity Concerns Rise as a Risk Factor for Board Members and Senior Executives in 2015.” [Online]. Available: http://www.prnewswire.com/news-releases/cybersecurity-concerns-rise-as-a-risk-factor-for-board-members-and-senior-executives-in-2015-300032571.html. [Accessed: 18-Apr-2015].

[5] “Internet Security Threat Report.” Symantec, 2015.

[6] “Frequently Asked Questions Learn more about the cyber attack against Anthem.” .

[7] “Banks: Credit Card Breach at Home Depot — Krebs on Security.” .

[8] “JPMorgan Chase Hacking Affects 76 Million Households,” *DealBook*. [Online]. Available: http://dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/. [Accessed: 23-Apr-2015].

[9] S. Perez, “Target’s Data Breach Gets Worse: 70 Million Customers Had Info Stolen, Including Names, Emails And Phones,” *TechCrunch*, 10-Jan-2014. .

[10] “What is CIA Triad of Information Security? - Definition from Techopedia,” *Techopedia.com*. [Online]. Available: http://www.techopedia.com/definition/25830/cia-triad-of-information-security. [Accessed: 20-Apr-2015].

[11] “Compliance - Covering Your Bases,” *AtNetPlus, Inc.* [Online]. Available: http://atnetplus.com/compliance-covering-your-bases/. [Accessed: 20-Apr-2015].

[12] W. S. Humphrey, *Managing the software process*, 28. print. Boston: Addison-Wesley, 2002.

[13] “What is competitive advantage? definition and meaning,” *BusinessDictionary.com*. [Online]. Available: http://www.businessdictionary.com/definition/competitive-advantage.html. [Accessed: 14-May-2015].

[14] M. E. Porter, *Competitive advantage: creating and sustaining superior performance: with a new introduction*, 1st Free Press ed. New York: Free Press, 1998.

[15] “Competitive Advantage.” .

[16] R. Holland, “Five Steps To Build An Effective Threat Intelligence Capability.” 15-Jan-2013.

[17] “Guide to Enterprise Risk Management.” Protiviti.

[18] “Threat vs Vulnerability vs Risk | Digital Threat.” .

[19] Sentrillion, “Safeguarding your information with a ‘Defense in Depth’ architecture.” .

[20] J. Pescatore, “2014 Trends That Will Reshape Organizational Security.” SANS Institute, Mar-2014.