ABSTRACT

Information security is an ever-growing field that requires constant attention in just about every industry today. Our study analyzes information security breaches that occur in companies using data envelope analysis (DEA). In particular, we applied a DEA model with constant returns-to-scale, which could handle undesirable outputs such as information security breaches, to the data set. When we controlled industry capital, we found that the retail financial/banking industries were relatively inefficient for dealing information security breaches. The major limitation of this study is the availability of data on security breaches. Further studies are necessary for in-depth analyses.

KEYWORDS: Privacy and security, Network security, Data envelopment analysis

INTRODUCTION

Information security is an ever-growing field that requires constant attention in just about every industry today. This is especially true in industries where dealing with non-public customer information is a regular occurrence. Staying on the cutting edge in this field is crucial to insure your information does not fall into the wrong hands. ISO (the International Organization of Standardization) just scratches the surface of current practices in place: There has been a vast amount of studies in this realm, but this is just the beginning of a long and arduous journey in properly securing the futures information. The expansion of knowledge is paramount to insure the integrity of a company's security measures. The continual research in the field of information security creates a wealth of new ideas regarding various methodologies to strengthen the security around sensitive information. When this subject falls to the wayside within a company, issues arise similar to the recent breach incident at Target. This incident is when upwards of 40 million individual’s credit and debit card information was obtained but an outside source (Target, 2015). The incident is one of the worst possible scenarios that can occur for an organization. The incident causes doubt within their customers: Now, they must go through inconvenient
steps to rectify the security breach on their own behaves, even if the incident is just for peace of mind. Ultimately, the incident can cause a loss in your customer base.

Policies have already been put in place to create a standard for information security, one of the most common being ISO 27000, which is a set of standards that help organizations keep information assets secure. Using this family of standards will help organizations manage the security of assets such as financial information, intellectual property, employee details or information entrusted by third parties (ISO, 2015). This standard includes many steps in defining the scope of your ISMS (Information Security Management System), establishing a structure and so on. A process such as this will constantly evolve throughout the projects life due to the nature of the subject.

Having the proper steps in place to insure the valuable information remains under wraps is an integral part of any business, and the constant development of these processes should be a routine part of a company’s strategy. New research and forward thinking is basis of improving information security. The rest of this study consists of literature review, results, discussion, and conclusion.

LITERATURE REVIEW

Alberts and Dorofee (2002) believed it was necessary to offer comprehensive information security risk evaluation, which included assessing assets, enabling decision making, the use of computing infrastructure, technological issues related to computing infrastructure, and flexible methods tailored to each organization. To carry out the risk evaluation, a specific set of requirements had to be created catering to these needs. Of course, these changes had to be actually implemented in order to be successful and should be the result of careful evaluation of the risk management approach of firms. Catteddu (2010) brought up an excellent consideration when it came to the cloud-computing portion of information security. Not only was it extremely important to be aware of these risks but also it was also crucial to be able to address them in a timely fashion. Whitman (2003) simply stated that a firm could more effectively construct security strategies by identifying and ranking the potential IS (information system) threats by severity. Anderson and Moore (2006) detailed the economics of information security. With the increased use of distributed systems, there were plenty of divergent interests, which were part of the process. This new field provided some valuable insight into both security topics and general areas of the design of these systems including optimal balance of effort by programmers and testers, why privacy got eroded, and the policies of digital rights management. Campbell et al. (2003) looked at the effect of information security breaches, which were reported in newspapers, or other publicly traded US corporations. There was limited evidence depicting the overall negative reaction to information security breaches. Upon further investigation, there was a highly significant negative reaction for breaches involving confidential data. These findings were consistent with the statement that economic consequences of the breach were different based on what the underlying assets of the breach were. According to Kotulic and Clark (2004), using a security risk management model (SRM) should provide a much more holistic view for a firm to use to assess their systems. However, research did not provide this proposed model. As defined by Solms (2004), there were 10 deadly sins that were consistently committed, which if not taken into consideration, would cause the security plan to fail. Management as a checklist to properly assess the security systems currently in place could use the sins defined in this study. Culgurcu, Cavusoglu, and Benbasat (2010) brought up an excellent point that one of the weakest links in information security was their employee. This study identified key points that would help employees adhere to specific information security policies (ISP). This study further described these key points that were a part of this process. Ultimately, the results showed that the key influencers to the bottom line of ISP were employees’ attitude, normative beliefs, and self-efficacy to comply. Solms (2001) clearly provided a detailed
multi-dimensional approach for information security as a discipline. This approach included but was not limited to information security, corporate governance, certification, awareness, and best practices. Solms (2005) also insisted the use of COBIT (Control Objectives for Information and Related Technology) and ISO 17799 as frameworks for the development of information security governance. This study focused on mapping out the similarities between these two models and addressing a certain degree of synchronization. Blakley, McDermott, and Geer (2001) emphasized addressing the use of information security technology to address a company exposed risk. This study only dealt with a small portion of the actual risk and might in fact be minimally effective in solving this risk. To solve this problem, an alternate model was proposed, which looking at the history of medicine developed. Brevard et al. (2015) in an audit conducted by the Office of the Inspector General (OIG) of the Chemical Safety Board’s (CSB) security practices, found several areas with room for improvement. They made several recommendations and pointed out that better managing practices related to information security planning, security controls, and vulnerability testing processes were vital to managing security risks. KPMG LLP (2014), an independent public accounting firm, conducted an audit on behalf of the U.S. Environmental Protection Agency’s (EPA’s) Office of Inspector General (OIG) and found that a lack of training left personnel without the skills and understanding necessary to identify, prevent, or lessen vulnerabilities affecting the EPA’s information systems and infrastructure. The audit found that “implementation of the EPA’s information security training program was hindered by inconsistent assignment of information security roles across the various EPA offices”. Safavi and Shukur (2014) conducted a study on improved conceptual framework for wearable health technology. This study included ten principles and nine checklists for providing complete privacy protection for mobile technology. Locasto et al. (2011) presented views on developing information security workers through education as opposed to mass certifications. They explored options such as funding cyber-security education, developing high-school pilot programs, providing guidance to ethical hackers, and expanding security specialties at universities. Puhakainen and Siponen (2010) suggested that their theory-based training of universal constructive instruction achieved positive results and was practical to implement. Additionally, they proposed that information security training should apply “contents and methods that activate and motivate learners to systematic cognitive processing of information received during training”. They also suggested that a continuous communication process was required to improve user IS security policy compliance. Kheirabadi, Kulkarni, and Shaligram (2011) discussed the idea of traffic monitoring within a wireless sensor network. Acknowledging that information technology (IT) systems were subject to security based threats like any other IT system. This approach should be considered an integral part of planning and deploying any system. Muktar (2014) elaborated on the subject of identifying mobile device requirements for user interface in social networking. What this study encompassed was the idea that mobile devices became essential tools in a person’s everyday life. Poorly designed systems could cause users to make significant errors, which attributed many software applications to never be properly utilized. Ultimately, a good design process would aid in solving these problems and that could encompasses GUI flaws to security issues alike. Humaidi and Balakrishnan (2015) used the idea of various leadership styles and IS compliance to play a role in security. Using surveys to gather data to back up a solid belief, the subject became clear that a big part of information security revolved around human errors. Better understanding the methods to improve the human errors would help the whole system. They also illustrated that it was not solely a technology-based subject. Waizumiet al. (2011) focused on network anomaly detection methods for improving efficiency and accuracy of information security. Discussing flow-based detection systems, which used packets to flow between transmissions, but within a large-scale network, was impractical. The recommended system could reduce the number of flows and reflect higher detection accuracy through various data sets and proposed methods. Ko and Dorantes (2006) conducted a study focusing on the impact of information security
breaches on the breached companies’ financial performance in the long-term following the announcement of a security breach. Their study proposed that such security breaches had significant immediate effects, but the long-term impacts were minimal. Cavusoglu, Mishra and Raghunathan (2004) conducted a study evaluating the immediate economic impact of Internet based security breaches. Their study found, while the market penalized all firms following a security breach, smaller firms were penalized more for security breaches than larger firms, and strictly Internet based firms were penalized most of all. Their findings also suggested that immediate responses to announced security breaches helped reduce the negative impact security breaches on firms’ capital. PWC (2015) conducted a very in-depth study on the global state of information security across many industries for 2015. This study resulted in detailed information generated for cybersecurity, hacks/incidents, and employees as the culprits of these incidents. This study laid out the key criteria contributing to this analysis, which all pointed to the importance of ensuring employees were working to prevent malicious attacks. Verizon (2015) also conducted a very detailed report surrounding the breaches which occurred in the industry. After conducting studies from 70 companies from 61 countries over 75,000 incidents were identified with over 2,000 confirmed breaches. The study went on to categorize the different types of breaches along with how they might be prevented. The finding was further categorized by industry as some companies were more susceptible than others to attacks.

In summary, there are many studies that focus on a range of topics associated with information security. The variety of different topics address frameworks and models to establish information security policies all the way to specific do’s and don’ts for protecting your assets. Due to the very wide nature of the subject, no one study addresses all of these topics. This paper hypothesizes that clear, manageable security policies, which employees can follow will greatly improve a company’s information security.

METHODOLOGY

In various industries of the economy, there are fluctuating levels of information based breaches, which span a variety of types and varies heavily on the type of industry. Overall, the most information sensitive industry will tend to have the most monetary damages, but not necessarily the most number of breaches. Based on PWC’s 2014 Survey (PWC, 2014) measuring cyber risks we deduce that most prevalent variables consist of the various breach types and the amount of breaches occurring each year. This approach can be broken down into various inputs and outputs. The input variables would be the industry capital and the percentage of each industry in the overall view.

The outputs include breaches by employee incidents, hackers, competitors and total damages. These all do not correlate to malicious intent based on some outside source attempting to access information, but can be as simple as an employee not following protocol and throwing out a piece of non-public customer information (NPCI), or leaving their laptop open in a coffee shop and having it stolen. However, breaches can be much more direct and can be results by hackers in various methodologies. No breach should be downplayed, as all policies are important, NPCI should be guarded and the protocol behind information security should be evolving regularly. Figure 1 shows our approach for analysis.

Figure 1: Research framework
Upon data collection, we use data envelopment analysis (DEA) for measuring the efficiencies of information systems for handling breaches and firms’ associated policies. DEA is an application of linear programming to measure the comparative efficiency of decision-making units (DMU). We use a DEA model with constant returns-to-scale, which can handle undesirable outputs. We treat information system breaches as undesirable outputs accompanied the use of information systems.

To explore the mathematical property of a basic DEA model, let $E_0$ be an efficiency score for the base DMU 0, then

$$
\text{Maximize } E_0 = \frac{\sum_{r=1}^{R} u_{r0} y_{r0}}{\sum_{i=1}^{I} v_{i0} x_{i0}} \tag{1}
$$

subject to

$$\left\{ \begin{array}{l}
\sum_{r=1}^{R} u_{r0} y_{rk} \\
\sum_{i=1}^{I} v_{i0} x_{ik}
\end{array} \right\} \leq 1 \text{ for all } k \tag{2}
$$

$u_{0r}, v_{0i} \geq \delta \text{ for all } r, i \tag{3}$

where

$y_{rk}$: is the observed quantity of output $r$ generated by unit $k = 1, 2, \ldots, N$,

$x_{ik}$: is the observed quantity of input $i$ consumed by unit $k = 1, 2, \ldots, N$,

$u_{0r}$: is the weight to be computed given to output $r$ by the base unit 0,

$v_{0i}$: is the weight to be computed given to input $i$ by the base unit 0, and

$\delta$: is a very small positive number.

The fractional programming model can be converted to a common linear programming (LP) model without much difficulty. First, move the numerator in Equation (1) to the side constraint
and set it equal to unity. Next, convert Equation (2) to a non-linear form by multiplying its numerator on both sides. The above model utilizes a constant returns-to-scale so that all observed production combinations can be scaled up or down proportionally (Charnes, Cooper, and Rhodes 1978).

Our sample data has been provided by surveys that PwC administered throughout 2013-2014, which broke down breaches by industry and further illustrated the types of breaches providing percentages and monetary figures by year. Analyzing the Bureau of Labor Statistics provided additional knowledge on how to properly breakdown the industries in the grand scheme if the world today providing an accurate average of workforce size and industry capital per area.

RESULTS

Table 1 exhibits data and variables we have analyzed. “Unity” is a standardized output variable to balance undesirable output variables. Accordingly, we include five variables in the model.

<table>
<thead>
<tr>
<th>Industry</th>
<th>Industry Capital ($)</th>
<th>No. of Employees</th>
<th>No. of Breaches by Hackers</th>
<th>No. of Breaches by Competitors</th>
<th>Unity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial</td>
<td>29,703.50</td>
<td>3,584</td>
<td>1,294</td>
<td>996</td>
<td>1</td>
</tr>
<tr>
<td>Retail</td>
<td>64,423.10</td>
<td>2,052</td>
<td>641</td>
<td>1,507</td>
<td>1</td>
</tr>
<tr>
<td>Medical</td>
<td>16,971.80</td>
<td>2,816</td>
<td>1,073</td>
<td>4,073</td>
<td>1</td>
</tr>
<tr>
<td>Industrial</td>
<td>33,703.20</td>
<td>1,272</td>
<td>553</td>
<td>615</td>
<td>1</td>
</tr>
<tr>
<td>Power</td>
<td>554.20</td>
<td>5,026</td>
<td>2,143</td>
<td>1,035</td>
<td>1</td>
</tr>
<tr>
<td>Variable Type</td>
<td>Input</td>
<td>Undesirable Output</td>
<td>Undesirable Output</td>
<td>Undesirable Output</td>
<td>Output</td>
</tr>
</tbody>
</table>

The first column indicates the industries represented in this study. Column two shows the each industry’s capital in millions of US dollars, or the cost to the industry of the breaches during the 2013 to 2014 time period. Columns three, four, five, and six indicate the various outputs representing the number of various breaches and incidents reported for each industry during 2013 to 2014.

Table 2 presents the descriptive statistics of continuous variables.

<table>
<thead>
<tr>
<th></th>
<th>Industry Capital ($)</th>
<th>No. of Employees</th>
<th>No. of Breaches by Hackers</th>
<th>No. of Breaches by Competitors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum</td>
<td>64,423.10</td>
<td>5,025.88</td>
<td>2,143.39</td>
<td>4,073.23</td>
</tr>
<tr>
<td>Minimum</td>
<td>554.20</td>
<td>1,271.62</td>
<td>533.26</td>
<td>615.30</td>
</tr>
<tr>
<td>Mean</td>
<td>29,071.16</td>
<td>2,950.05</td>
<td>1,137.03</td>
<td>1,645.23</td>
</tr>
<tr>
<td>Standard Deviation</td>
<td>21,124.52</td>
<td>1,292.43</td>
<td>574.77</td>
<td>1,246.57</td>
</tr>
</tbody>
</table>

The variables in Table 2 show high levels of variability across industries. Table 3 displays the correlation matrix of the continuous variables.
Table 3: Correlation between variables

<table>
<thead>
<tr>
<th></th>
<th>Industry Capital</th>
<th>No. of Employees Incidents</th>
<th>No. of Breaches by Hackers</th>
<th>No. of Breaches by Competitors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Industry Capital</td>
<td>1</td>
<td>-0.7082</td>
<td>-0.7930</td>
<td>-0.1673</td>
</tr>
<tr>
<td>No. of Employees Incidents</td>
<td>-0.7082</td>
<td>1</td>
<td>0.9842</td>
<td>-0.0189</td>
</tr>
<tr>
<td>No. of Breaches by Hackers</td>
<td>-0.7930</td>
<td>0.9842</td>
<td>1</td>
<td>-0.0509</td>
</tr>
<tr>
<td>No. of Breaches by Competitors</td>
<td>-0.1673</td>
<td>-0.0189</td>
<td>-0.0509</td>
<td>1</td>
</tr>
</tbody>
</table>

There is a very strong correlation between the number of breaches by hackers and the number of employee incidents. This indicates that as the number of breaches by hackers increases the number of employee incidents also increases. There are also two negative correlations represented by the data. The first shows that there is a fairly strong negative correlation between the number of employee incidents and industry capital. It means that as the number of incidents increases the amount of industry capital decreases, as companies have to pay more for the breach. The second negative correlation also shows that as the number of breaches by hackers increases the amount of money a company has decreases. Finally, there is a very weak negative correlation between industry capital and the number of competitor breaches, which means that if one company has a breach than other companies may be likely to lose money as well. Table 4 includes efficiency scores and ranks.

Table 4: Efficiency scores and ranks

<table>
<thead>
<tr>
<th>Rank</th>
<th>DMU</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>POWER/UTILITIES</td>
<td>1.0000</td>
</tr>
<tr>
<td>1</td>
<td>INDUSTRIAL</td>
<td>1.0000</td>
</tr>
<tr>
<td>1</td>
<td>MEDICAL/HEALTHCARE</td>
<td>1.0000</td>
</tr>
<tr>
<td>4</td>
<td>BANKING/CREDIT/FINANCIAL</td>
<td>0.5753</td>
</tr>
<tr>
<td>5</td>
<td>RETAIL/CONSUMERS</td>
<td>0.4292</td>
</tr>
</tbody>
</table>

The numbers in the first column represent the ranking of each DMU based on their corresponding efficiency scores in the third column. The efficiency scores in column three can be between 0 and 1, meaning 0 is not efficient at all, and 1 is 100 percent efficient. The results of Table 3 indicate that during the time period of 2013 to 2014 the Power and Utilities, Industrial, and Medical/Healthcare industries operated relatively at 100 percent efficiency; meaning that the number of breaches for each did not outweigh the cost of each breach. The Banking/Credit/Financial and Retail/Consumers industries were relatively less efficient, indicating significant costs with each breach. See Figure 5 for graphical representation of each industry’s efficiency.
The overall data shows the various correlations, and efficacies between the industries and the types of breaches used as output. This will ultimately allow for a meaningful analysis of the state of the policies in place and how effective this is for the industry.

DISCUSSION

The findings of this study support the hypothesis that clear, manageable security policies which employees can follow will greatly improve a company’s information security. This finding is also supported in the literature review, particularly in studies by Alberts and Dorofee (2002), Ko and Dorantes (2006), and Cavusoglu, Mishra, and Raghunathan (2004).

Alberts and Dorofee (2002) study considers appropriate methods for evaluating information security risks. Suggesting beginning with the organization itself, rather than from the “bottom-up”, for companies to determine what needs to be protected and why it is at risk, and from there develop effective policies and procedures. The study included a vulnerability evaluation showing organizations needed to feel “ownership” and more involved in security processes and policy developments. Our findings further confirm Alberts and Dorofee’s evaluation by showing the correlation between loss of industry capital and the number of security breaches. As the number of breaches increases, so do the costs incurred by each industry as well as decreased trust investors and consumers have in that industry. This negative correlation displays how after major security breaches, investors and consumers lose faith in the ability of that industry to protect information causing those industry losses in revenues.

In a study conducted by Ko and Dorantes (2006) information security breaches’ long-term affects proved to be insignificant. Their results suggested that while there were significant decreases in revenues the quarter immediately following an announced security breach, the long-term economic impact was minimal. They attributed these findings to firms responding quickly and appropriately with additional security measures to prevent future breaches and that as time passes people move on and ecommerce continues. Our findings support their results showing the immediate costs associated with each industry and the number of incidents. For example, the number of total incidents by employees, hackers, and competitors for the power
industry is higher than the rest but the total industry capital costs are the lowest of the studied industries.

Cavusoglu, Mishra, and Raghunathan (2004) revealed in their study that announcing an Internet security breach is negatively associated with the market value of the announcing firm. The firms they studied showed that breached firms lost an average of 2.1 percent of their market value within the two days surrounding the events, a $1.65 billion average loss in market capitalization per incident. Their study also explained the estimated losses directly related to investors’ expectations about the impact on future cash flows and anticipation of future breaches. Additionally, their findings showed that the market penalized all firms for security breaches and particularly Internet firms. The findings of our study support Cavusoglu et al. (2004) with the displayed negative correlation between each industry and industry capital. As the number of security incidents increase the respective industry capital decreases.

The managerial implications of this study propose that increased education and training of employees will lead to fewer security breaches and increases in industry capital through the reduction of costs associated with breaches. Our study revealed that the highest number of security incidents for each industry was a direct result of employees, whether malicious or accidental. This result implies that with additional training of employees, clear and manageable policies and procedures, and continuous improvement of security measures firms can have a direct and positive impact on their capital.

CONCLUSION

In summary, our study focused on conducting an analysis of the number of information security breaches that occur in companies. Leveraging a data envelope analysis (DEA) model, the analysis focused on categorizing information by industry and contained several inputs and outputs. The inputs included the size of the industry represented by workforce percentage and industry capital represented in million US dollars. Major industries reviewed consisted of banking, retail & consumers, medical, industrial, and power and utilities. Organizing the breaches by category, which included human error, hacking, and competition, also segmented the data. The outputs were depicted as the damages in US dollars and the sheer number of breaches experienced. After running the DEA analysis, some interesting results were uncovered. For one, industry and hack types do not have to be one in the same. In addition, a strong negative correlation was identified between the number of breaches by hackers and the amount of industry capital, which means that as breaches go up the amount of capital the company has, goes down. For the same reasons described previously, there was also a strong negative correlation between the number of employee incidents and the amount of industry capital. The last interesting fact identified was that three industries tied for the highest relative efficiency score of 1. Power/utilities, industrial, and medical/healthcare all displayed that the number of breaches for each industry didn’t outweigh the cost each caused.

Because this study is exploratory in nature, there should be further studies. The first is conducting a more tactical look at very specific companies within each industry to further segment these broader categories. The second is to gather consistent data from employees who adhere to company policies to gauge the effectiveness of their security awareness training. The last, DMUs would be to review the amount invested by companies into their IT security departments and how effective they were in preventing or mitigating breaches. Additional studies conducted on this subject should dive deeper into the details and collect more comprehensive information on employee adherence to policies. Diving deeper into what specific companies have spent to prevent breaches would offer a much more focused view into what causes many of these breaches to occur and what companies are doing to respond.

Acknowledgement
Alex Heinen and Tera Black, graduate students at Central Connecticut State University MBA Program, contributed to this study.

REFERENCES


