2019

Data Security Threats Sources: An Empirical Examination of Institutional Characteristics

Nasim Talebi

Emmanuel Wusuhon Yanibo Ayaburi

Suhail Chakravarty

Chapter 6
Data Security Threats Sources: An Empirical Examination of Institutional Characteristics

Nasim Talebi
University of Texas at San Antonio, USA

Emmanuel Ayaburi
University of Texas Rio Grande Valley, USA

Suhail Chakravarty
University of California – Santa Barbara, USA

ABSTRACT

Driven by the difficulty in achieving complete security with technical tools, business investigators are looking into organizational and behavioral issues that could help make systems more secure. This chapter looks at the security of systems from the organizational perspective. Specifically, this study attempts to identify if different organizations have different predisposition to particular type(s) of security threat sources. Using publicly available security breach data from a privacy rights clearinghouse to investigate which organizational characteristics predisposes an institution to an external or internal threat source, it was concluded that as size of organization and the number of its valuable documents increase by one unit, the organization's probability of suffering an internal attacks decrease. Furthermore, when executive members have a business degree rather than information-security-related degrees, the likelihood of suffering an internal attack increases. Also, the probability of an organization suffering an internal or external attack is not based on its industry type.

DOI: 10.4018/978-1-5225-5393-9.ch006

INTRODUCTION

Acts that affect the integrity and availability of business information systems as well as the privacy of business data threatens the security of those information systems. To achieve a secured system, the information systems must be protected from unauthorized access, use, disclosure, disruption, modification or destruction. As organizations continue to depend on complex information systems, the identification of sources of threat to these systems are very important (Warkentin & Willison 2009). Organizations of different types and sizes have different information security threats that they need to be aware of to ensure their sensitive information and assets are protected. The 2010/2011 Computer Security Institute's Computer Crime and Security Survey of 351 computer security practitioners revealed that most organizations experienced relatively less system security breaches over the years but the attacks are increasingly complex with some successful breaches resulting in huge financial loss (Warkentin & Willison 2009).

Prior studies on recent breaches have categorized potential sources of threats including cracking, malicious code, falsification and physical assault (Warkentin & Willison 2009). Another study developed a scoring system for vulnerabilities that pose threats to the systems. Some other studies which focused on the individuals within the organization, have suggested that individuals are the most important factor in protecting an information systems (Workman, Bommer, & Straub 2008).

Internal actors, according to findings by McAfee research, account for 43% of data loss and thus is a significant part of data loss. In the same study, they found that 68% of these incidents were significant enough to have a financially negative impact on the enterprise or firm (McAfee 2017). This means that insider threat and its financial consequences are issues that must be addressed and prevented for a company to succeed.

The threat of a data breach from an insider can come in multiple forms and have varying levels of dangers. A study by the Ponemon Institute in 2017 found in a survey of 874 incidents that the money lost from and the frequency of each type of insider breach. The data in the table adapted from a Ponemon Institute Infographic shows a comparison of insider breaches categorized under Malicious Insider, Negligent Insider, and Credential Theft. See Table 1.

Table 1. Adapted from Ponemon Institute 2016 infographic report: DTEX, 2017

Breach Type	% of Incidents	Cost to Contain	Annualized Cost
Malicious Insider	22%	$347,130	$1,227,812
Negligent Insider	68%	$206,933	$2,291,591
Credential Thief	10%	$493,093	$776,165

From the data presented, the Ponemon Institute concluded that although Credential Theft were the most expensive to contain, Negligent Insiders costed the most by sheer volume of incidents caused by human error. Given that 30% of data breaches that have negative financial impacts are insider breaches, it can be said that insider threat is a problem that firms must attempt to mitigate. In order to gain an understanding of the gravity of the problem, one must gain an understanding of how much it costs a firm to suffer an insider attack.

Insider Threat Cost Analysis and Examples

While it may seem that the containment of data breaches are the extent of the costs of a leak, there are many more underlying factors to the costs of an internal breach. Here are above the surface costs which are better known, as well as below the surface costs which might be less visible. Deloitte in an analysis of data breaches gave a list of above and below the surface consequences.

Some above the surface costs are:

- Technical Investigation
- Customer Breach Notification
- Regulatory Compliance
- Attorney Fees and Litigation
- Post Breach consumer protection
- Public relations
- Cybersecurity Improvements

While the below the surface costs are:

- Insurance Premium Increases
- Increased Cost to Raise Debt
- The Impact of Operational Disruption or Destruction
- Value of Lost Contract Revenue
- Devaluation of Trade Name
- Loss of Intellectual Property
- Lost Value of Customer Relationships

List adapted from Deloitte Infographic (Mossburg et al. 2016)

Using the caveats between the type of breaches and the opportunity cost, the costs of insider breaches can be explained with the different aspects of the price due to insider threat and are best illustrated using real world examples of insider breaches.

Stories of Costly Insider Breaches

Woolworths Negligent User Insider Breach

In another costly breach of data, the grocery store Woolworths lost a significant amount of money from an unintentional loss of data from an authorized user. GroupOn and Woolworths teamed up to sell "e-gift cards" at a discounted price and the customer would receive a voucher code to redeem for the Woolworths store credit. When customers were supposed to receive the pdf for their gift card, they instead received an email with a link to a spreadsheet that had the emails of thousands of customers and voucher codes that added up to $1,308,505. Opportunistic customers took advantage of the blunder and quickly redeemed both their own vouchers as well as those of other customers.

Many customers had their gift cards used before they were able to redeem it and as one customer reported, his gift card was used in a city 300km away (Reilly 2015).

The disclosure of voucher prices and customer emails was not a malicious attempt but rather was a result of negligence that not only resulted in financial loss but also resulted in a loss of customer satisfaction (Reilly 2015; Visentin 2015). Woolworths has agreed to refund the customers that have had their vouchers stolen but will lose all the money that had been stolen and used as a result of this debacle.

In the aftermath of the breach, Woolworths has to make investments beyond the reimbursement of customers. This would include retraining all the employees in better data management, notifying customers of the breach, and the below the surface

Australian Government Leak

The G20 summit is a meeting among world leaders from 19 of the largest world countries and the European Union. Being one of the most high profile events, the data available to the organizers is the most coveted and sensitive pieces of information in the world. Attendees included Vladimir Putin from Russia, President Barack Obama, President Xi Ping, and Prime Minister Narendra Modi (Farrel 2015). For the sake of efficiency, the immigration department must have access to all of the attendees' passport numbers, date of births and visa numbers. Given the valuable information to the immigration department, one would expect employees to err on the side of caution. However, that was not the case.

An employee, in an email, was meant to send these highly valued pieces of information to a colleague. However, the Australian government uses Microsoft Outlook which has an autofill function for email addresses. In a critical blunder, an employee of the Australian Immigration Department sent the email to the wrong person as a result of the autofill function. The passport numbers, among other vital

pieces of information, of 31 international leaders attending the summit were sent to a member of the local organizing committee for the Asia Cup football tournament.

Given that this information was not spread further to the public by the recipient of the email, there was a comparatively tame effect on those whose information was compromised. The real problem stemmed from the government's reaction to the breach. None of the world leaders or their teams were notified of the breach until well after the issue had occurred. Just weeks before the leak, Australian government officials were urging citizens to trust them with personal data but after the blunder, Australian citizens were rightfully hesitant.

The costs as a result of the breach stemmed from public relations costs, retraining costs, and system improvements.

Financial Analysis of AT&T Malicious Insider Breach

One example of Insider Attacks that costed the firm a significant amount was an attack on the telecommunications giant AT&T between November 2013 and April 2014. In this time, call center employees from Mexico were paid by third parties to obtain and release customer information used to attempt to open stolen cell phones (Chabrow 2015). AT&T allows for cell phones to be fully unlocked for customers by asking for the customer's name and the last four digits of the customer's social security number with the expectation that only the customer and AT&T would have access to that data. However, with hopes of reselling the unlocked phones, the third party attempted to take advantage of the unlocking system by paying employees of call centers for names and Social Security Numbers. After gaining this information, the ring of cell phone thieves made 290,803 handset unlock requests with the information that had been compromised (National Cybersecurity Institute 2016).

Upon this incident, AT&T was forced to publicize its occurrence upon which the Federal Communications Commission launched its own investigation into the event. During the FCC's investigation, it was found that the three call center employees in Mexico gave information for 68,000 accounts. However, the FCC exposed further breaches taking place in Colombia and the Philippines. In the Colombian and Philippine facilities, an additional 40 employees had accessed 211,000 customer accounts (Federal Communications Commission 2015).

After the results of the investigation, the FCC took its biggest enforcement action by fining AT&T $25 million as well as requiring that all customers be notified, pay for credit monitoring services for customers affected by breaches in Colombia and Philippines. On top of the financial consequences, AT&T was required increase security by appointing a privacy certified senior compliance manager, conduct a privacy risk assessment, implement regular employee training and file compliance reports for the FCC (Federal Communications Commission 2015).

In order to fulfill the FCC's wishes, the fine was not the only cost AT&T suffered from the breach. According to Zurich Insurance Company, notifying a customer costs an average of $2.75, thus, that the cost of notifying the 279,000 account owners would come out to be $767,250 (Bailey 2014). According to the Ponemon Institute the cost of containment would cost at least $2.83 million for an average breach size of 24,089. Since the AT&T breach was 11½ times larger than the average breach, the cost of containment would be at least $32 million (Chabrow 2015). The cost to improve general security measures for a company with over 200,000 employees such as AT&T can be estimated at $70 million according to Deloitte (Mossburg et al. 2016). The total tangible costs of the AT&T breach thus comes out to be $128 million dollars. However, according to both Deloitte and the Kaspersky Institute, there are intangible losses and financial impacts such as customer loss and lost contracts as a result of the insider breach(Mossburg et al. 2016; Kaspersky 2015). Thus the loss that AT&T suffered as a result of the data breach in call centers is even larger than the tangible direct costs of the breach.

Why Is This Important?

While some of the costs from an insider breach are apparent, there are many hidden aspects that must be evaluated. Both malicious and negligent insiders can be trained or filtered with better training and awareness that could save a significant amount of money for any firm that is a target. Getting better insurance and training would cost the firm significantly less as is made clear by Philip Lieberman, president of IT security provider Lieberman Software, when he says "The cost to implement a control would be one-tenth - or vastly less - of the cost of the fine and other losses" (Ponemon 2017). The cost of insider breaches is undeniable and so is the necessity of better protection against the attacks given the financial and business consequences that come with insider threats. Identifying the factors that play into the susceptibility of a company is the ideal way to prevent such an attack.

However, due to resource constraints, organizations are not able to implement unlimited technical controls to protect their systems. Instead, they need to understand the major threat (external or internal) that systems will likely face so as to implement effective controls accordingly. This understanding stems from a 'self-awareness' about the respective type of industry and size of the firm as well as other additional factors.

This study attempts to identify if different organizations have different predisposition to particular type(s) of security threat. The ability to identify vulnerabilities will guide any investment of resources into protecting assets most likely to suffer an attack. Based on the review of past literature we developed four hypotheses which relate the firm size, industry type, Information Technology

(IT) competence and firm knowledge to external or internal types of threat. These hypotheses were tested empirically with security breach data gathered from Privacy Rights Clearinghouse and S&P Capital IQ providing company information. Following a statistical analysis of 35 reported security breaches using logistic regression, it was realized that as size of organization, reflected in the number of employees, increases, and as the amount of firm knowledge assets, reflected in the number of documents, the organization's probability of suffering an internal attacks decreases relative to external attacks. Also, the probability of suffering an internal attack relative to external attack for executives' business degree holders is higher. No statistically significant differences in threat source across industries was found in our analysis.

In subsequent sections, we will review the literature related to the subjects of information security threats and organizational factors. Then present the research model and hypotheses derived, outline the research methodology, report the results of the model testing, and discuss the findings and their theoretical and managerial implications. Then conclude with a discussion about the limitations and directions for future research.

BACKGROUND AND LITERATURE REVIEW

Categorization of breaches and mitigation strategies or techniques have been the predominant theme in most research. One such theme is the human factor and its influence on threat categories. A longitudinal study, (Warkentin & Willison 2009) found that the proportion of threat due to physical, false, malicious and cracking vulnerability categories have remained relatively stable over the years. Thus concluding that human error has been undervalued and should be regarded as a significant factor in protecting information systems. Herzog et al (2007) developed a web Ontology Language-based model which includes asset, threat, vulnerability, countermeasure and security goal and defense strategy as its core concepts. A general category of security threat sources introduced by Krausz (Chang & Ho 2006) hypothesizes that the actions a firm can take to prevent incidents depends on who, where and what the source of attack is. Given this hypothesis, four different categories of threats were devised: external versus internal, unintentional versus intentional, manual versus automatic, and human versus nature. Most researchers classify threats to information system security into two broad categories of external and internal (Workman & Bommer 2008). In addition, Al-Zubi (2010) is of the opinion that sources of threats can be divided into two internal and external classes, depending on the type of media used. Threats can then further be classified into groups depending on their location from the point of vulnerability.

An attempt to develop a vulnerability scoring systems for information systems has also been of interest to researchers. Mell et al. (2006) developed a common security scoring systems that generates consistent scores of vulnerabilities. Systems with higher scores need to be mitigated proactively. Some mitigation factors focus on the human dimension such as education and awareness of employees and third parties (Workman & Bommer 2008). Omissions and careless behavior by users threaten the security of most information systems. Workman et al. (2008), in an attempt to find out why there is omission of security measures among employees who should know the importance of securing a system, suggested that perceived severity of consequences employees will suffer from a breach influences how motivated they are to prevent breaches. Some other sources of threats include natural disasters, organization procedure and computer virus (Loch, Carr, & Warkentin 1992). This study extends from prior studies as it takes a focus on organizations' features and how those features influence these organizations' predisposition to either an internal or external attack on its information system.

STUDY OF POTENTIALS FACTORS THAT AFFECT SUSCEPTIBILITY

Issues, Controversies, Problems

Some of these threats sources include hostile cyber/physical attacks, human error or omission or disasters due to natural or man-made occurrence (Mell, Scarfone, Romanosky 2006). This study focuses on the first two sources since the third, disasters, affects all industries and there is little by way of effort organizations can do to prevent them from happening or predicted their occurrence. Threats due to attacks are usually carried out by adversaries who are not with the organization but are attempting to disrupt operation for either financial gain or for the joy of it. For the purpose of this study those types of threats sources are referred to as external threat sources while threats due to human omission or commission within the organization for any reason will be referred to as internal threats sources. One key factor in risk analysis is the consequence or assets that are affected (Chang, Ho 2006). Different organizations vary in the size and sensitivity of the assets they have. Therefore the type of threat source can be motivated by factors including type of target organization, the size of target organization, academic security knowledge of executive team members and the amount of precious documents. Next will be a discussion of these factors and their relationship to potential threat source.

1. Industry Type

Industry sector has been used in many previous research related to information security management and end-user security behavior (Ghobadian and Gallear 1997; Taylor and McGraw 2004; Stanton et al. 2005). Organizations have different needs for information systems in their operations. For some organizations, lack of availability of their information system means disruption in the provision of their services or products. These differences in information systems need appeal differently to different attackers since the attacker communities are not homogenous. For example, the attractiveness of a financial institution to an external attack by a hacker community is different compared to a non-profit organization. This is because there will be different type of challenges to the effort of an attacker and the attackers also benefit differently. A multi industry study in Korea revealed that there is differences across industries in the categories of information system security threats they face such that manufacturing considers interruption more serious, while academia and distribution firms considers modification and interruption more serious (Chang & Ho 2006). Therefore an organization's use of IT is influenced by the type of industry it operates in making organizations to be exposed to kinds of security threat. Thus we hypothesize that:

Hypothesis One: The industry type an organization operates in influences the source of security threat to its information system.

2. Organizational Size

Organizations in different sizes tended to handle information security differently with different levels of available resources and expertise (David 2002). While small organizations are generally resource poor and more sensitive to outside pressure (Ghobadian and Gallear 1997), larger ones encounter a problem due to the nature of the organization which is the more number of employees. Loach et al. (1992) are of the opinion that employees and organizational procedures are a greater threat to the security of information system infrastructure compared to other factors. As an organization increases in size the number of employees and documents produced increases. The likelihood of security breaches due to the number of employees also increases and makes the impact of the human element more pronounced. The human element is often referred to as the weakest link in the chain of security defense of information system. Possible ways to control for this factor is to create security awareness among employees or monitor their activities constantly. Employee compliant work practices are important to the security of IT operation. Therefore organizations must implement monitoring mechanisms to ensure compliance or

detection of non-complaint behavior. With regard to these two remedies, larger companies have a tendency to underestimate the value of building awareness (Krausz 2015). In addition, the larger the firm the larger the cost involve in monitoring and securing the IT infrastructure. Therefore when the organization increases in size the human factor is more pronounced since the number of people to monitor on the network increases. Some employee work practices that have been identified as increasing the risk of a system includes resistance to adopting initiatives to improve security (Chang & Ho 2006). However, complete monitoring of employees might not be possible and managers cannot predict the intent of all employees. Hence we hypothesize that:

Hypothesis Two: The size of an organization influences the source of information system security threat such that large organizations are prone to internal attacks than small organizations do.

3. IT Competence

Information Technology (IT) competence makes it possible for a company to plan, organize, execute, and invest on information security effectively (DTEX 2017). More specifically, it is "the set of IT-related knowledge and experience that a business manager possesses" (Bassellier et al. 2003). It has been found in previous literature that the IT competence of business managers not only positively influence their attitudes toward practicing security controls and management (Bassellier et al. 2001; Hagen et al. 2008), but also makes them have proactive Information Security Management behaviors (Hagen et al. 2008). Majoring in IT or security related fields, executive managers can understand the necessity of allocating security investment budgets at the first place. Then, the need for building security awareness in employees through training programs along with focusing on employees as a potential threat to the overall security of systems are more understandable for them. Hence:

Hypothesis Three: IT competence of executive managers influences the source of security threat to its information system.

4. Firm Knowledge

Organizations are more dependent than ever on information systems (IS) to enhance business efficiency and effectiveness. Therefore, protecting those systems are of importance to organizations. However, most of the time the focus is only on either corporate computer assets or corporate IT systems, and information asset and data protection is utterly underestimated. Therefore, those information assets that

organizations have makes them more attractive to outsiders such that the greater the size of the documents and the depth of data, the more hackers interested in. Not only outsider, but also insiders will become attracted to those knowledge assets. Park & Ho (2006) found that insiders have caused great damage and loss to corporate internal information assets. Hence:

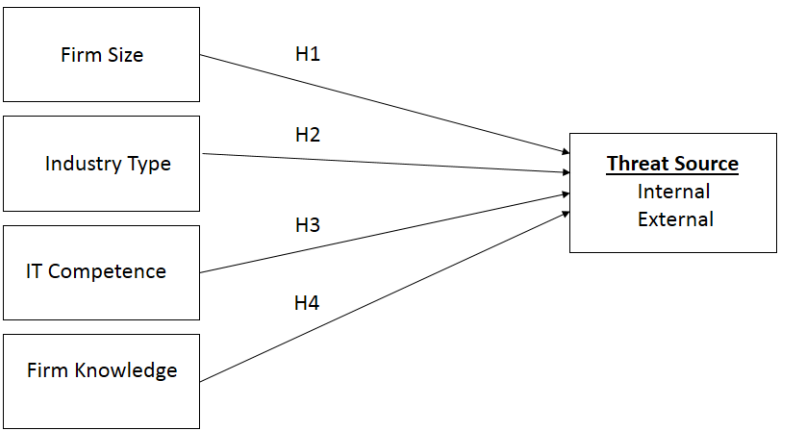
Hypothesis Four: The total number of documents an organization have influences the source of information system security threat.

METHODOLOGY

Data

To study the research model depicted in Figure 1, we chose an empirical study approach using security breaches reported in the US as described below. An empirical methodology for this study is a good choice since evidence is needed to support the above hypothesis. Although the threat sources to information systems are varied, this study is concern about institutional factors that influence the type of threat source. Factors of interest are size of an organization, the industry type, IT competence of executive members, and firm knowledge. Data used to test the above hypotheses were obtained from Privacy Rights Clearinghouse's (PRC) repository of data breaches reported in the US along with S&P Capital IQ providing information on companies worldwide. Although 4669 breaches were reported from March 2005 to November 2015, not all breaches were usable because there were no reports

Figure 1. Research model



about the type of breach that occurred or the number of potential documents being accessed by fraudsters. After deletion of such data, the study ended up with 2211 useful observations for further analysis. Among those 2211 breaches we just were able to collect complete data for 41 organizations and focus on 35 of them to do hypotheses testing. Table 2 shows the descriptive statistics of the data.

Variables

Source of threat variable has two dimensions; internal and external threat source. External threat source are those breaches which can be traced to an individual or system outside the organization. Privacy Rights Clearinghouse reports the type of breaches on its website. For this study external threat sources are data breaches resulting from hacking or stealing of portability devices by third parties outside the organization. Internal threat sources on the other hand are those threats that can be traced to the actions of individuals within the organizations. Such threats include unintended disclosure, insider breach, loss of company information assets and employees falling for the activities of fraudster.

The size of the organization, which was measured using the number of employees, determines its exposure level to attackers. In fact, organizational total assets and revenue can also be used to represent the size of an organization. However, we use the number of employees because we believe human factors have great influence in determining an organization's security threats.

The type of industry an organization firm is in was based on the categories of organizations by PRC. In all seven categories were reported covering business, finance, education, health, not for profit and government. This categorization in the opinion of the author covers nearly all industries and the study therefore adopted their

Table 2. Data distribution

Threat Score Frequency	Percent
External 17	48.57
Internal 18	51.43
Total 35	100
Industry Type	
Financial 14	40
Medical 14	40
Others 7	20
Total 35	100

Table 3. Variables

Variable Name	Definition
Internal Threat (Internal)	Threat which is as a result of an action by an individual within the firm. These include unintended disclosure, insider breach and loss to fraudsters.
External Threat (External)	Breaches traced to an individual or system outside the organization. These include hacking and stealing by third parties.
Organizational Size (Trfirmsize)	Natural log of the total number of employees in an organization.
Industry Type (Industrytype)	Main type of activity carried out in the breached firm.
IT Competence (Majoruse)	Academic major the executive team hold.
Firm Knowledge (Trknowledgeasset)	Natural log of the total number of documents in an organization.

categorization. Due to the lack of data points in various industries, we used two main industries including financial coded as 1, medical coded as 2, and other industries coded as 3. The other category have instances from not for profit organizations, retail, and government institutions. The reference category used for analysis was the financial organization category. And since the continuous predictor variable of firm size, and firm knowledge were highly positively skewed, we used natural log transformation to make data ready for the analysis.

Results Analysis and Discussion

First proposed in the 1970s as an alternative technique to overcome the limitations of ordinary least squares regression in handling dichotomous outcomes, logistic regression analysis was used to predict the probability that a cyber-attack on a firm would come from an internal source relative to an external source.

A test of the final model with threat source as the dependent variable and firm size, industry type, IT competence, and firm knowledge as predictor variables compared with only the constant included null model was statistically significant with a Chi, $X^2 = 25.450$ with $p < 0.05$. Table 4 shows the logistic regression coefficient, Wald test, and odds ratio for each of the predictors. The odds and probability of an internal attack for each industry type is shown in Table 4 as well. Employing a 0.10 criterion of statistical significance, knowledge assets, firm size and IT competence of executive members were found to be significant.

One unit increase in firm size, the odds of suffering from an internal (1) attack decreases by (0.578-1)*100% = 42%. Also, the probability of getting an internal

Table 4. Variables in the Equation

Variables in the Equation

		B	S.E.	Wald	df	Sig.	Exp(B)	95% C.I.for EXP(B)	
								Lower	Upper
Step 1[a]	Trknowledgeasset	-.415	.238	3.050	1	.081	.660	.415	1.052
	Trfirmsize	-.549	.249	4.863	1	.027	.578	.355	.941
	Industrytype			2.911	2	.233			
	Industrytype(1)	-2.469	1.515	2.657	1	.103	.085	.004	1.649
	Industrytype(2)	-2.258	1.530	2.178	1	.140	.105	.005	2.097
	Majoruse			4.054	2	.132			
	Majoruse(1)	3.401	1.689	4.054	1	.044	29.981	1.095	821.032
	Majoruse(2)	-17.159	40192.970	.000	1	1.000	.000	.000	.
	Constant	5.362	2.786	3.704	1	.054	213.242		

a. Variable(s) entered on step 1: Trknowledgeasset, Trfirmsize, Industrytype, Majoruse.

attack when the executive member holds a business degree is 29.98 times or 70% higher comparing to those who have IS degrees. In addition, one unit increase in the number of documentation, the odds of suffering from an internal attack decreases by (0.66-1)*100= 34%.

Thus, the data support H1 in a reverse direction, along with H3 and H4 in the predicated direction at the 10% significance level. However, the probabilities for an internal attack are not statistically different across financial, medical and other types of industries. The result of hypotheses testing is provided in Table 5.

Table 5. Results

	Hypotheses	**Result**
H1	*The* ***size*** *of an organization influences the source of information system security threat such that large organizations are prone to internal attacks than small organizations.*	**Supported - reverse**
H2	The **industry type** an organization operates in influences the source of security threat to its information system.	**Not supported**
H3	**IT competence** of executive managers influences the source of security threat to its information system.	**Supported**
H4	*The* **total number of documents** *an organization have influences the source of information system security threat.*	**Supported**

FUTURE RESEARCH DIRECTIONS

The results of this study should be interpreted with caution since there are many limitations to this study. First of all, the small sample size used in this study was the biggest concern of the authors. In addition, the use of reported breaches might not truly reflect the number and types of breaches organizations actually encounter as some organizations might be unwilling to disclose any news about a breach due to the impact it will have no its reputation.

Also, nearly half of the observations in the PRC data set were unusable due to the lack of information with regard to attack categorization. For instance, either the number of documents accessed or a potential source of attack was not made known as reported in the sample section of the methodology. Proper classification of these breaches and their inclusion in the analysis might potentially alter the results obtained in this study. In addition, since the sample is limited to the United States of America, it is suggested to replicate this study in other countries to reconfirm the result before using its implications. Finally, no interaction effect between the independent variables was examined. The interaction of those factors might impact the overall results obtained in this study. Future studies will exam the interactive effect of firm size and industry type.

CONCLUSION

Organizations face constant attacks on their information systems infrastructure and the data that they keep on a daily basis. These attacks could originate from an outside entity such as a hackers or actions and omissions from insiders who have privileged access to the systems. This study sought to investigate if the industry an organization belongs to, its size in terms of number of employees, the IT skills and knowledge of its executive member(s), or organization knowledge in the form of the amount of valuable documentation predisposes one organization to an internal attack relative to an external attack. Based on reviews of previous literature, the study investigated four hypotheses which state that the size of firm, along with the magnitude of documentations and academic knowledge and expertise of executive level are positively associated with its likelihood of suffering an internal attack and that the source of attacks vary by industry type. Following an execution of binary logistic regression on data set on publically announced security breaches, it was realized that larger organizations are not necessarily prone to internal attacks. Instead, smaller companies seem to be more prone to internal cyber attacks. A possible explanation for this is that while bigger companies probably face more internal attacks, these are more often successful in smaller companies due to a lack of investment in cyber

attack prevention. This then makes one wonder if larger organizations are prone to external attacks instead. This unanswered question will be investigated in the future. However, the source of threat or an attack does not seem to differ across industries. In other words, firms experiencing internal threat source have fewer number of documents and are smaller in size, while their executive members hold a business degree versus an Information System or Information Security related degree.

This study highlights some concerns for managers in practice. The conclusion of this study appears to suggest that as firm become larger, they become attractive targets for hackers and thieves looking to the firm's assets.

ACKNOWLEDGMENT

This research was supported by National Science Foundation under grant number 1724725. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

REFERENCES

Al-Zubi, A. A. (2010). *Identification of Information Systems Threats Sources: An Analytical Study*. Academic Press.

Ashibani, Y., & Mahmoud, Q. H. (2017). Cyber physical systems security: Analysis, challenges and solutions. *Computers & Security*, *68*, 81–97. doi:10.1016/j.cose.2017.04.005

Bauer, S., & Bernroider, E. W. (2017). From information security awareness to reasoned compliant action: Analyzing information security policy compliance in a large banking organization. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, *48*(3), 44–68. doi:10.1145/3130515.3130519

Chabrow, E. (2015, April 18). Insider Breach Costs AT&T $25 Million. In *GovInfoSecurity*. Skybox Security. Retrieved from www.govinfosecurity.com/insider-breach-costs-att-25-million-a-8089

Chang, S. E., & Ho, C. B. (2006). Organizational factors to the effectiveness of implementing information security management. *Industrial Management & Data Systems*, *106*(3), 345–361. doi:10.1108/02635570610653498

Colwill, C. (2009). Human factors in information security: The insider threat – Who can you trust these days? *Information Security Technical Report*, *14*(4), 186–196. doi:10.1016/j.istr.2010.04.004

Crossler, R. E., Bélanger, F., & Ormond, D. (2017). The quest for complete security: An empirical analysis of users' multi-layered protection from security threats. *Information Systems Frontiers*, 1–15.

Evesti, A., Kanstrén, T., & Frantti, T. (2017, June). Cybersecurity situational awareness taxonomy. In *Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), 2017 International Conference On* (pp. 1-8). IEEE.

Federal Communications Commission. (2015). Available at https://apps.fcc.gov/edocs_public/attachmatch/DOC-332911A1.pdf

Giovinazzi, S., Brown, C., Seville, E., Stevenson, J. R., Hatton, T., & Vargo, J. J. (2016). Criticality of infrastructures for organisations. *International Journal of Critical Infrastructures*, *12*(4), 331–363. doi:10.1504/IJCIS.2016.081303

Herzog, A., Shahmehri, N., & Duma, C. (2007). An ontology of information security. *International Journal of Information Security and Privacy*, *1*(4), 1–23. doi:10.4018/jisp.2007100101

Hu, Q., Hart, P., & Cooke, D. (2007). The role of external and internal influences on information systems security – a neo-institutional perspective. *The Journal of Strategic Information Systems*, *16*(2), 153–172. doi:10.1016/j.jsis.2007.05.004

Hurlburt, G. (2016). Good Enough" Security: The Best We'll Ever Have. *Computer*, *49*(7), 98–101. doi:10.1109/MC.2016.212 PMID:28003687

Im, G. P., & Baskerville, R. L. (2005). A longitudinal study of information system threat categories: The enduring problem of human error. *ACM SIGMIS Database*, *36*(4), 68–79. doi:10.1145/1104004.1104010

Initiative, J. T. F. T., & ... (2009). *800-53 Rev. 3*. SP: Recommended Security Controls for Federal Information Systems and Organizations.

Jung, B., Han, I., & Lee, S. (2001). S. Security threats to Internet: A Korean multi-industry investigation. *Information & Management*, *38*(8), 487–498. doi:10.1016/S0378-7206(01)00071-4

Kaspersky Lab. (2015). *Damage Control: The Cost of Security Breaches IT Security Risks Special Report Series*. Retrieved from https://media.kaspersky.com/pdf/it-risks-survey-report-cost-of-security-breaches.pdf

Krausz, M. (2015). *Managing information security breaches: Studies from real life. S.l.* IT Governance Ltd.

Loch, K.D., Carr, H.H., & Warkentin, M. E. (1992). Threats to Information Systems: Today's Reality, Yesterday's Understanding. *MIS Quarterly, 16*(2), 173.

Mell, P., Scarfone, K., & Romanosky, S. (2006). Common vulnerability scoring system. *IEEE Security & Privacy, 4*(6), 85–89.

Mossburg, E. (2017, September 15). *Beneath the surface | Deloitte US | Cyber Risk Services*. Retrieved November 17, 2017, from https://www2.deloitte.com/us/en/pages/risk/articles/hidden-business-impact-of-cyberattack.htm

Moteff, J. C. (2005). Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities and Consequences. *American Journal of Hospital Pharmacy*, *47*(3), 533–543.

National Cybersecurity Institute. Excelsior College. (2016, July 11). *Insider Breach Costs AT&T $25 Million*. Retrieved from www.nationalcybersecurityinstitute.org/telecommunications/insider-breach-costs-att-25-million-2/

Peppard, J., & Ward, J. (2016). *The strategic management of information systems: Building a digital strategy*. John Wiley & Sons.

Ponemon Institute. (2017). *Cost of Data Breach Study*. Available at www.ibm.com/security/data-breach/index.html

Posey, C., Raja, U., Crossler, R. E., & Burns, A. J. (2017). Taking stock of organisations' protection of privacy: Categorising and assessing threats to personally identifiable information in the USA. *European Journal of Information Systems*, 1–20.

Reilly, C. (2015, May 31). *Data breach sees Woolworths gift cards leaked in email bungle*. Retrieved November 17, 2017, from https://www.cnet.com/au/news/data-breach-sees-woolworths-gift-cards-leaked-in-email-bungle/

Richardson, R. (2011). *2010/2011 Computer Crime and Security Survey*. Retrieved from http://gatton.uky.edu/FACULTY/PAYNE/ACC324/CSISurvey2010.pdf

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, *36*(2), 215–225. doi:10.1016/j.ijinfomgt.2015.11.009

Stewart, H., Stewart, H., Jürjens, J., & Jürjens, J. (2017). Information security management and the human aspect in organizations. *Information & Computer Security*, *25*(5), 494–534. doi:10.1108/ICS-07-2016-0054

DTEX Systems. (2017). *The True Price Tag of Insider Threats: Findings from the New 2016 Cost of Insider Threats Report*. Retrieved from dtexsystems.com/true-price-tag-insider-threats-findings-new-2016-cost-insider-threats-report.

Thompson, M. (2016). *Harmonised Taxonomies of Security and Resilience: A Suitable Foundation for the Security Discipline* (Doctoral dissertation). University of New South Wales, Canberra, Australia.

van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., & Kusev, P. (2017). Risk perceptions of cyber-security and precautionary behaviour. *Computers in Human Behavior*, *75*, 547–559. doi:10.1016/j.chb.2017.05.038

Visentin, L. (2015, May). Woolworths Leaks $1 Million of Gift Cards in Massive Data Breach Debacle. *The Sydney Morning Herald.* Retrieved from www.smh.com.au/digital-life/consumer-security/woolworths-leaks-1-million-of-gift-cards-in-massive-data-breach-debacle-20150530-ghd8wl.html

Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: The insider threat. *European Journal of Information Systems*, *18*(2), 101–105. doi:10.1057/ejis.2009.12

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, *24*(6), 2799–2816. doi:10.1016/j.chb.2008.04.005