Journal of the Midwest Association for Information Systems (JMWAIS)

Volume 2016 | Issue 1 Article 4

2016

Enterprise Computer Security: A Literature Review

Dennis C. Acuña
Dakota State University, dcacuna@bright.net

Journal of the Midwest Association for Information Systems

Volume 2016 | Issue 1 Article 3

Date: 01-30-2016

Enterprise Computer Security: A Literature Review

Dennis C. Acuna

Dakota State University, dcacuna@dsu.edu

Abstract

Information technology (IT) is a global phenomenon that provides organizations of all types the ability to achieve enterprise objectives. One IT component is computer security, sometimes referred to as cybersecurity, the detection and prevention of a rapidly evolving collection of threats and vulnerabilities capable of introducing significant IT risk to an organization. Seminal events such as the creation of U.S. Cyber Command in 2009 acknowledging cyberspace as the fifth domain of war, and the 2015 recall by Fiat Chrysler of 1.4 million vehicles to mitigate an Internet enabled threat, serve as bookends framing the rapid evolution of cybersecurity threats and the need for organizations to better understand the collective vulnerabilities that enable computer security risk. However, a recent literature review of a major information systems (IS) research journal suggests publication of academic research associated with management of computer security from an enterprise perspective is limited. Given the relevance of computer security in today's IT environment, this finding suggests that enterprise computer security is an under studied research topic. This article addresses this finding and the research gaps with the intent of encouraging new research in this domain.

Keywords: Enterprise computer security, cybersecurity, IT governance, literature review.

1. Introduction

Given that computer threats may cause widespread disruption to enterprise stability, computer security has evolved from a back office discussion to a recurring topic of interest at the highest levels of senior management. To effectively mitigate modern computer threats it is necessary to understand the collective vulnerabilities that increase computer security risk from an enterprise perspective, and address computer security comprehensively, as opposed to managing computer security as a series of discrete computer vulnerabilities. Developing such an approach is critical to ensure the achievement of enterprise objectives and to maintain enterprise sustainability (B. von Solms, 2001b).

Although it remains possible for organizations to manage their affairs without the use of modern technology, few managers choose to do so. Given the ready availability of information technology (IT) that enables data collection, data management, and data sharing at low cost, high speed, and reduced human error, modern organizations leverage IT to remain competitive within the industry in which they compete. As suggested by Porter's Five Forces model, the availability of commercial-off-the-shelf (COTS) IT permits the smallest organization to achieve IT economies of scale that enable rivalry against larger competitors (Porter, 1979, 1980, 1985). Also, the phenomenon of low cost, readily available IT has lowered the barrier of entry across many industries, as COTS IT empowers organizations of all types with the ability to compete more aggressively on a more equal footing to achieve enterprise objectives (Carr, 2003, 2004, 2005).

While the skillful implementation of IT aligned with organizational requirements enables the achievement of enterprise objectives, the ease with which IT can be implemented is not without liability. In fact, the ease with which IT can be deployed can be viewed as a modern day version of the sirens' song, in that implementation of IT includes acceptance of risk that may or may not be immediately visible to the adopting organization. Some of this risk is manifested in the form of data breaches and the leakage of sensitive information, while an increased likelihood of risk impacting other vulnerabilities is incurred if due care and due diligence are not taken into consideration (Gerber & von Solms, 2001; Gerber & von Solms, 2005; Gerber & von Solms, 2008; Liang & Xue, 2009; R. von Solms & von Solms, 2006).

Managerial failure to understand the vulnerabilities associated with IT can lead to organizational ineffectiveness, in that failure to manage IT risk decreases an organization's ability to achieve enterprise objectives and maintain enterprise sustainability (Goldstein, Chernobai, & Benaroch, 2011). In regard to managing the vulnerabilities that enable IT risk, the technology known as the Internet of Things (IoT) has been identified by the National Intelligence Council as one of six disruptive technologies with the power to spread IT risk far more widely than the Internet has to date. Given the need for effective and uninterrupted IT to achieve enterprise objectives and to maintain enterprise sustainability, the strategic focus of IT has shifted from maximizing IT competitive advantage to minimizing IT vulnerabilities. Thus, the study of comprehensive computer security from an enterprise perspective represents a current challenge of significant interest to the manager of any organization that relies on IT as a strategic organizational component (National Intelligence Council, 2008; B. von Solms, 2001a; B. von Solms & von Solms, 2005; R. von Solms & van Niekerk, 2013).

This article defines the problem of enterprise computer security, reviews the articles on the topic in a major information systems journal, identifies research gaps and needs, and discusses limitations and conclusions.

2. Problem Definition and Motivation

Early computer security objectives focused on common vulnerabilities associated with the identity and access management use cases of user authentication, user authorization, and physical access to computing assets. Over time, vulnerabilities associated with the security triad of confidentiality, integrity, and availability (CIA) were identified and mitigated, as computer security evolved into a more comprehensive model. However, the recent realization of the Internet, the World Wide Web, and the Internet of Things has introduced a new era of computer threats that are unprecedented in scale and scope, and continue to show signs of rapid evolution.

Seminal events such as the 2009 government decision to create U.S. Cyber Command acknowledging cyberspace as the fifth domain of war, and the 2015 business decision by Fiat Chrysler to recall 1.4 million vehicles to mitigate an Internet enabled threat, serve as bookends framing the rapid evolution of computer threats and the need for organizations to better understand and manage the vulnerabilities that enable computer security risk (Anonymous,

2010; Greenberg, 2015; U.S. Army Cyber Command, 2015; Vijayan, 2009). One way to gauge the evolution of computer security risk is to observe the frequency of data breaches (Figure 1). Recent data breaches associated with Heartland, Citigroup, Adobe, Target, Home Depot, Staples, Sony Pictures Entertainment, Anthem, and the Office of Personnel Management (OPM), among others, help underscore the likelihood of a data breach occurrence (Privacy Rights Clearinghouse, 2015). Another way to gauge the evolution of computer security risk is to observe the change in sophistication of computer threats (Figure 2) from low level hacking attacks, to coordinated nation state cyberattacks using weaponized software such as the Stuxnet worm, the first piece of malware known to target and destroy physical assets (Zetter, 2011).

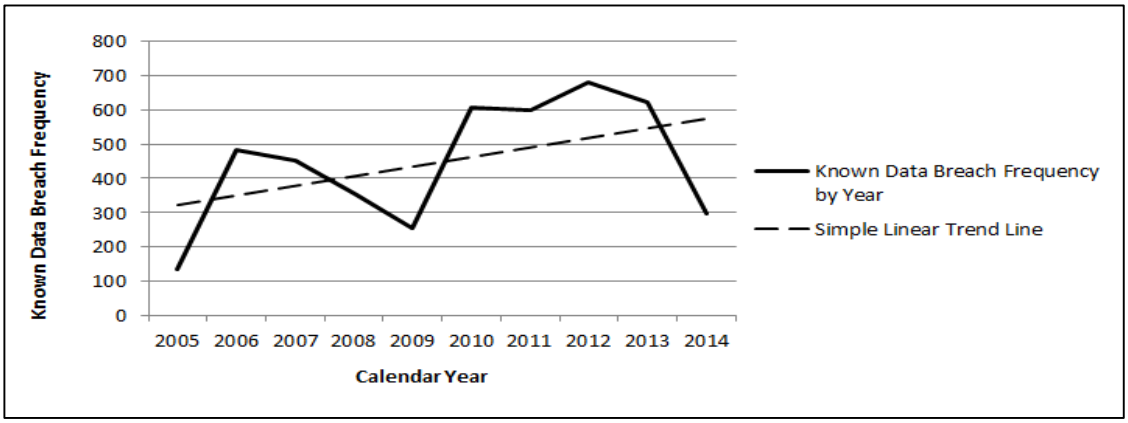

Figure 1. Known Data Breach Frequency by Calendar Year

Figure 1 is a graphical representation of the frequency of known data breach activity over the calendar years 2005 through 2014 (Privacy Rights Clearinghouse, 2015). Calendar year 2015 is not included in Figure 1 as data for 2015 was not complete at the time this manuscript was being prepared. Known data breach frequency is represented in Figure 1 by a solid black line, representing the number of known data breaches for a given calendar year. Trending is represented by a dotted black line, calculated as a simple linear trend line of the known data breaches per year. By examining Figure 1, we observe that the frequency of known data breaches is trending upward, an observation that is supported by the reporting of data breach activity in the public press.

Figure 2 is a composite representation of the evolution of computer threat sophistication based upon various practitioner resources referenced from the public domain (Ponemon Institute, 2015; PwC, 2015; Verizon, 2015). Figure 2 depicts the relative increase in computer security risk over time, based on the increasing sophistication of computer threats. Beginning with hacking activity associated with kiddie scripts and hacktivists, computer threats have evolved into industrial espionage and the current state of affairs characterized by leaders of sovereign nations engaged in diplomatic discussion to mitigate nation state cyberattacks. By examining Figure 2 in conjunction with what is reported in the public press, we can surmise, as have practitioners, that the evolving sophistication and risk associated with computer threats is increasing, not decreasing.

Whereas early forms of computer security risk resulted in the loss of computing capability, the ongoing sustainability of the enterprise was never really a concern. The advent of the Internet, the World Wide Web, and the Internet of Things, coupled with the paradigm of organizational reliance on IT to sustain industry competitiveness, now threatens that outlook given the need for a strong enterprise computer security posture to avoid the loss of IT prowess (Da Veiga & Eloff, 2007; Mata, Fuerst, & Barney, 1995; McFadzean, Ezingeard, & Birchall, 2007; National Intelligence Council, 2008; H. A. Smith & McKeen, 2009). In today's operating environment, organizational failure to understand and manage enterprise computer security from a comprehensive perspective increases the likelihood that an organization will fail to meet one or more of its objectives, or fail to maintain ongoing sustainability. Thus, effective governance of enterprise computer security is critical for the achievement of enterprise objectives, and for maintaining enterprise sustainability (Merhout & O'Toole, 2015a). To ensure effectiveness, computer security must be recognized by senior management as a critical component of enterprise risk management (Posthumus & von Solms, 2004; Van Niekerk & Von Solms, 2010; B. von Solms, 2001a; Westerman & Hunter, 2007).

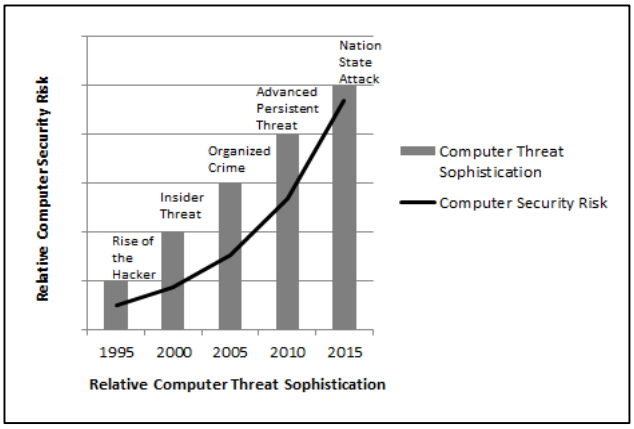

Figure 2. Evolution of Computer Threats

Thus, computer security represents an important part of IT. A recent literature review of the information systems research journal MIS Quarterly (MISQ) suggests that publication of academic research associated with a comprehensive understanding of computer security from an enterprise perspective is somewhat in short supply. This finding suggests that the comprehensive study of enterprise computer security is an under studied research topic. The remainder of this article addresses this finding and the research gaps therein, with the intent of encouraging new research in this domain.

3. Literature Review

Based on a working hypothesis that research associated with the comprehensive study of computer security from an enterprise perspective is somewhat limited, a literature review was performed for the purpose of discovering relevant academic research associated with enterprise computer security.

Computer security is a broad topic. To avoid boiling the ocean and to better guide this initial research effort, a decision was made to limit this literature review to a single journal and a specific publication time frame in order to quickly gauge the academic work product that represents enterprise computer security. The journal selected was MIS Quarterly, its editorial objective being "the enhancement and communication of knowledge concerning the development of IT-based services, the management of IT resources, and the use, impact, and economics of IT with managerial, organizational, and societal implications" (MIS Quarterly, 2015). The publication time frame selected was 2009 to 2015, an interval associated with seminal computer security events from a practitioner perspective, most notably the creation of U.S. Cyber Command in 2009 and the Fiat Chrysler recall in 2015.

One reason for selecting MISQ as the lone journal for this literature review was to provide a relatively quick benchmark and proxy for relevant mainstream IT research on this topic, given MISQ's membership in the Association for Information Systems (AIS) Senior Scholars' Basket of Journals, as shown in Table 1 (Association for Information Systems, 2015). Another reason for selecting MISQ was to establish the framework for a future opportunity to repeat this research methodology on the other academic journals that make up the Senior Scholars' Basket of Journals, as well as other academic journals that publish manuscripts on computer security research. Increasing the scope of this literature review in a follow-up study will provide additional evidence to support or disprove the working hypothesis that research associated with the comprehensive study of computer security from an enterprise perspective is somewhat in short supply.

For this literature review, relevant academic research is defined as research that contributes to the comprehensive understanding and management of computer security from an enterprise perspective, such that it improves organizational ability to achieve enterprise objectives and maintain enterprise sustainability.

Table 1. AIS Senior Scholars' Basket of Journals, in Alphabetical Order

Row	Journal Name
1	European Journal of Information Systems
2	Information Systems Journal
3	Information Systems Research
4	Journal of AIS
5	Journal of Information Technology
6	Journal of MIS
7	Journal of Strategic Information Systems
8	MIS Quarterly

4. Methodology

The gross list of candidate articles for this literature review was identified using the AIS eLibrary search tool as the primary search mechanism. The AIS eLibrary search tool was chosen due to its intuitive user interface, fast performance, and a handy sorting feature for viewing search results by year. Keyword searches were performed against MISQ journal entries using relevant computer security search phrases constructed from the keywords enterprise, computer, security, cybersecurity, information, assurance, and governance.

The time frame for each search was set to a start date of 2009, the year U.S. Cyber Command was created, and an end date of 2015, the year of the Fiat Chrysler 1.4 million vehicle recall, thereby framing discovery to the period of time deemed relevant to the practical observation of computer vulnerabilities exposed to modern computer threats. In regard to MISQ publishing nomenclature, each search period began with MISQ volume 33 issue 1 (March 2009) and ended with MISQ volume 39 issue 2 (June 2015).

Using the list of articles returned by each search, a PDF version of each document and its associated metadata was exported from the Business Source Premier online database repository and stored in EndNote version X7.4. Business Source Premier was also used to determine the number of MISQ articles published per issue. Two editing passes were then made through the list of retrieved articles. The first editing pass served to clean the gross list of candidate articles by identifying duplicate titles and non-research titles. Duplicate titles are defined as the same article returned by more than one keyword search, and non-research titles are defined as content representative of comments, opinions, essays, introductions, or other material not representative of a research article. The second editing pass served to cull and categorize the cleaned list of remaining candidate articles in preparation for content analysis. An Excel worksheet was used to log the statistics and metadata resulting from each editing pass, and for building the figures and tables presented in this article. Content analysis followed the completion of the second editing pass.

4.1 First Editing Pass – Cleaning Process

As shown in Table 2, a gross total of 227 candidate articles were discovered using combinations of the keywords selected for this literature review. Initial analysis (Table 3) of the gross candidate articles revealed 71 duplicate titles, and the identification of 31 titles deemed to be non-research as defined above. Removal of the duplicate titles and non-research titles from the gross total yielded a net total of 125 candidate research articles, which were then compared against the MISQ publication pattern for the time frame being measured (Table 4).

Table 4 shows the distribution of the 370 total articles published by MISQ between volume 33 issue 1 and volume 39 issue 2, compared to the 125 net candidate articles retained for the second editing pass. Examination of Table 4 reveals that the first pass at identifying relevant research articles resulted in the selection of 33.78% of the 370 total articles published by MISQ between volume 33 Issue 1 and volume 39 Issue 2, an average of 17.86 articles per year. This finding suggests that on average, slightly more than one-third of the articles published by MISQ on an annual basis between 2009 and 2015 were associated with some facet of computer security from an enterprise perspective. While promising, the second editing pass of this analysis does not support this statement.

Table 2. Gross Candidate Articles Returned, by Year, by Keyword Search

Keyword Search Results	Totals	2009	2010	2011	2012	2013	2014	2015
computer cybersecurity	**6**		2		2	1		1
computer security	**86**	7	16	15	15	12	12	9
enterprise cybersecurity	**2**				2			
enterprise security	**35**	4	8	3	5	6	7	2
governance	**60**	5	5	7	11	18	6	8
information assurance	**38**	3	4	4	11	8	4	4
Totals	**227**	**19**	**35**	**29**	**46**	**45**	**29**	**24**

Table 3. Articles Deemed Non-Relevant, by Year

Non-Relevant Search Results	Totals	2009	2010	2011	2012	2013	2014	2015
duplicate title	**71**	6	15	6	14	14	8	8
non-research	**31**		5	4	8	5	5	4
Totals	**102**	**6**	**20**	**10**	**22**	**19**	**13**	**12**

Table 4. Number of Articles Published by MISQ, by Year, by Issue, Compared to Net Candidate Articles

Vol 33 Iss 1 thru Vol 39 Iss 2	Totals	2009	2010	2011	2012	2013	2014	2015
March	**99**	14	10	13	18	16	15	13
June	**96**	10	11	13	15	21	14	12
September	**87**	12	11	15	19	15	15	
December	**88**	12	11	15	18	17	15	
Totals	**370**	**48**	**43**	**56**	**70**	**69**	**59**	**25**
net candidate articles	**125**	13	15	19	24	26	16	12
Percent of Total	**33.78%**	**27.08%**	**34.88%**	**33.93%**	**34.29%**	**37.68%**	**27.12%**	**48.00%**

4.2 Second Editing Pass – Categorizing Process

Following the first pass cleaning process, each of the 125 net candidate articles was examined for its contribution to comprehensive computer security from an enterprise perspective, as opposed to research describing computer security from the perspective of a discrete subject devoid of having an enterprise impact. As shown in Table 5, 23 of the 125 net candidate articles from Table 4 were categorized as relevant research articles, in that each article communicates computer security research findings from a comprehensive, enterprise perspective. In other words, each of the MISQ articles listed in Table 5 addresses a facet of computer security from a comprehensive, enterprise perspective, as opposed to portraying a facet of enterprise computer security in the form of a discrete subject unrelated to the larger body of computer security controls that constitutes an enterprise computer security defense-in-depth model.

Table 6 summarizes the research categorization of each article in Table 5 by calendar year. Other than a total of seven computer security articles published in 2010, which happens to align with the rise of U.S. Cyber Command, Table 6 shows no significant patterns of interest. Furthermore, there is no empirical evidence to link this observation with a statement of substance.

While the first editing pass suggested that slightly more than one-third of the articles published by MISQ on an annual basis between volume 33 Issue 1 and volume 39 Issue 2 included some facet of enterprise computer security (Table 4), the results of the second editing pass shown in Table 7 do not support that observation. Instead we observe that only 6.22% of the 370 total MISQ articles, an average of 3.29 articles per year, are associated with some form of computer security from a comprehensive, enterprise perspective. This is interesting in that despite the methodology used to pull MISQ articles from the AIS eLibrary, some of the net candidate articles proved to have minimal connection to computer security (Rai, Pavlou, Im, & Du, 2012), while others that did focused on computer security from a discrete perspective (Dey, Lahiri, & Guoying, 2014).

Thus, the second editing pass resulted in the identification of 23 relevant research articles from the starting

pool of 125 net candidate articles, as shown in Table 5 and Table 7. Each of the relevant research articles selected for content analysis was deemed to have met the criterion that the research contributes to the comprehensive understanding and management of computer security from an enterprise perspective, such that it improves organizational ability to achieve enterprise objectives and maintain enterprise sustainability.

4.3 Content Analysis

To ensure a strong computer security posture that will protect the enterprise against the loss of IT prowess, it is imperative that organizations develop a comprehensive understanding of the computer threats and vulnerabilities unique to their organization, and the practical solutions that reduce computer security risk. The need for a comprehensive understanding of computer security from an enterprise perspective compared to a niche understanding of individual computer security components is necessary to ensure that all of the interlocking components of a computer security program are recognized, understood, and managed as a whole, as opposed to managing discrete components of a fragmented computer security model. Failure to manage computer security from a comprehensive enterprise perspective leads to a false sense of security, and little reduction in overall computer security risk (B. von Solms, 2001b; Zuccato, 2004, 2007).

Each of the 23 relevant research articles (Table 5) selected for this content analysis meets this criterion. A synthesis of the relevant research articles follows.

Humans are the weakest link in computer security. Organizational development of a training and awareness program as a means of managing the human aspect of computer security is a critical step in building a solid foundation for an enterprise computer security program. Current, well established threats target human vulnerability in the form of low-cost threat vectors capable of penetrating high-cost defenses. Phishing emails are one example. Phishing emails sent to key personnel represent computer threats capable of penetrating a network perimeter. In 2014 the German government announced that a spear-phishing attack targeted the corporate network at a German steel mill. The attack was successful in gaining access to industrial control systems to the point that a blast furnace could not be properly shut down, resulting in significant damage to the plant (Zetter, 2015).

Another low-cost threat is the use of a USB flash drive, or memory stick, to inject malware into an end-point device within a network perimeter. The 2010 revelation of the Stuxnet worm served to validate the effectiveness of the USB port as a low-cost threat vector. Insider threat activity in the form of a disgruntled worker performing harmful actions against the organization is also a low-cost threat vector. The 2010 Bradley Manning release of U.S. Army classified information to WikiLeaks, followed by the 2013 Edward Snowden release of National Security Administration (NSA) classified information to various media outlets, both serve as benchmarks of the organizational impact of insider threat activity. When properly conducted, training and awareness programs provide an effective control for mitigating the computer security risk that exists in the human component of the people, process, technology

Table 5. MISQ Relevant Research Articles, by First Author

Row	Year	Categorization	MISQ Journal Citation
1	2010	compliance	Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). INFORMATION SECURITY POLICY COMPLIANCE: AN EMPIRICAL STUDY OF RATIONALITY-BASED BELIEFS AND INFORMATION SECURITY AWARENESS. MIS Quarterly, 34(3), 523-A527.
2	2011	network vulnerability	Chen, P.-y., Kataria, G., & Krishnan, R. (2011). CORRELATED FAILURES, DIVERSIFICATION, AND INFORMATION SECURITY RISK MANAGEMENT. MIS Quarterly, 35(2), 397-A393.
3	2009	privacy	Culnan, M. J., & Williams, C. C. (2009). HOW ETHICS CAN ENHANCE ORGANIZATIONAL PRIVACY: LESSONS FROM THE CHOICEPOINT AND TJX DATA BREACHES. MIS Quarterly, 33(4), 673-687.
4	2014	creating value	Fichman, R. G., Dos Santos, B. L., & Zheng, Z. (2014). DIGITAL INNOVATION AS A FUNDAMENTAL AND POWERFUL CONCEPT IN THE INFORMATION SYSTEMS CURRICULUM. MIS Quarterly, 38(2), 329-A315.

5	2010	creating value	Gordon, L. A., Loeb, M. P., & Sohail, T. (2010). MARKET VALUE OF VOLUNTARY DISCLOSURES CONCERNING INFORMATION SECURITY. MIS Quarterly, 34(3), 567-A562.
6	2012	outsourcing	Gupta, A., & Zhdanov, D. (2012). GROWTH AND SUSTAINABILITY OF MANAGED SECURITY SERVICES NETWORKS: AN ECONOMIC PERSPECTIVE. MIS Quarterly, 36(4), 1109-A1107.
7	2009	offshoring	Hahn, E. D., Doh, J. P., & Bunyaratavej, K. (2009). THE EVOLUTION OF RISK IN INFORMATION SYSTEMS OFFSHORING: THE IMPACT OF HOME COUNTRY RISK, FIRM LEARNING, AND COMPETITIVE DYNAMICS. MIS Quarterly, 33(3), 597-616.
8	2010	training & awareness	Johnston, A. C., & Warkentin, M. (2010). FEAR APPEALS AND INFORMATION SECURITY BEHAVIORS: AN EMPIRICAL STUDY. MIS Quarterly, 34(3), 549-A544.
9	2015	training & awareness	Johnston, A. C., Warkentin, M., & Siponen, M. (2015). AN ENHANCED FEAR APPEAL RHETORICAL FRAMEWORK: LEVERAGING THREATS TO THE HUMAN ASSET THROUGH SANCTIONING RHETORIC. MIS Quarterly, 39(1), 113-A117.
10	2014	governance	Juhee, K., & Johnson, M. E. (2014). PROACTIVE VERSUS REACTIVE SECURITY INVESTMENTS IN THE HEALTHCARE SECTOR. MIS Quarterly, 38(2), 451-A453.
11	2012	forecast accuracy	Li, C., Peters, G. F., Richardson, V. J., & Weidenmier Watson, M. (2012). THE CONSEQUENCES OF INFORMATION TECHNOLOGY CONTROL WEAKNESSES ON MANAGEMENT INFORMATION SYSTEMS: THE CASE OF SARBANES-OXLEY INTERNAL CONTROL REPORTS. MIS Quarterly, 36(1), 179-204.
12	2009	training & awareness	Liang, H., & Xue, Y. (2009). AVOIDANCE OF INFORMATION TECHNOLOGY THREATS: A THEORETICAL PERSPECTIVE. MIS Quarterly, 33(1), 71-90.
13	2011	creating value	Mithas, S., Ramasubbu, N., & Sambamurthy, V. (2011). HOW INFORMATION MANAGEMENT CAPABILITY INFLUENCES FIRM PERFORMANCE. MIS Quarterly, 35(1), 237-256.
14	2015	privacy	Park, I., Sharman, R., & Rao, H. R. (2015). DISASTER EXPERIENCE AND HOSPITAL INFORMATION SYSTEMS: AN EXAMINATION OF PERCEIVED INFORMATION ASSURANCE, RISK, RESILIENCE, AND HIS USEFULNESS. MIS Quarterly, 39(2), 317-A319.
15	2013	insider threat	Posey, C., Roberts, T. L., Lowry, P. B., Bennett, R. J., & Courtney, J. F. (2013). INSIDERS' PROTECTION OF ORGANIZATIONAL INFORMATION ASSETS: DEVELOPMENT OF A SYSTEMATICS-BASED TAXONOMY AND THEORY OF DIVERSITY FOR PROTECTION-MOTIVATED BEHAVIORS. MIS Quarterly, 37(4), 1189-A1189.
16	2010	compliance	Puhakainen, P., & Siponen, M. (2010). IMPROVING EMPLOYEES' COMPLIANCE THROUGH INFORMATION SYSTEMS SECURITY TRAINING: AN ACTION RESEARCH STUDY. MIS Quarterly, 34(4), 767-A764.
17	2012	vulnerability management	Ransbotham, S., Mitra, S., & Ramsey, J. (2012). ARE MARKETS FOR VULNERABILITIES EFFECTIVE? MIS Quarterly, 36(1), 43-64.
18	2010	compliance	Siponen, M., & Vance, A. (2010). NEUTRALIZATION: NEW INSIGHTS INTO THE PROBLEM OF EMPLOYEE INFORMATION SYSTEMS SECURITY POLICY VIOLATIONS. MIS Quarterly, 34(3), 487-A412.
19	2010	compliance	Smith, S., Winchester, D., Bunker, D., & Jamieson, R. (2010). CIRCUITS OF POWER: A STUDY OF MANDATED COMPLIANCE TO AN INFORMATION SYSTEMS SECURITY DE JURE STANDARD IN A GOVERNMENT ORGANIZATION. MIS Quarterly, 34(3), 463-486.
20	2010	user participation	Spears, J. L., & Barki, H. (2010). USER PARTICIPATION IN INFORMATION SYSTEMS SECURITY RISK MANAGEMENT. MIS Quarterly, 34(3), 503-A505.
21	2015	compliance	Vance, A., Lowry, P. B., & Eggett, D. (2015). INCREASING ACCOUNTABILITY THROUGH USER-INTERFACE DESIGN

			ARTIFACTS: A NEW APPROACH TO ADDRESSING THE PROBLEM OF ACCESS-POLICY VIOLATIONS. MIS Quarterly, 39(2), 345-A348.
22	2013	governance	Williams, C. K., & Karahanna, E. (2013). CAUSAL EXPLANATION IN THE COORDINATING PROCESS: A CRITICAL REALIST CASE STUDY OF FEDERATED IT GOVERNANCE STRUCTURES. MIS Quarterly, 37, 933-A938.
23	2013	insider threat	Willison, R., & Warkentin, M. (2013). BEYOND DETERRENCE: AN EXPANDED VIEW OF EMPLOYEE COMPUTER ABUSE. MIS Quarterly, 37(1), 1-20.

IT triad (Bulgurcu, Cavusoglu, & Benbasat, 2010; Cole, 2014; Johnston & Warkentin, 2010; Johnston, Warkentin, & Siponen, 2015; Liang & Xue, 2009; Posey, Roberts, Lowry, Bennett, & Courtney, 2013; Puhakainen & Siponen, 2010; Spears & Barki, 2010; Willison & Warkentin, 2013).

Table 6. Enterprise Computer Security Research Categorization, by Year

Research Categorization	Totals	2009	2010	2011	2012	2013	2014	2015
compliance	5		4					1
creating value	3		1	1			1	
forecast accuracy	1				1			
governance	2					1	1	
insider threat	2					2		
network vulnerability	1			1				
offshoring	1	1						
outsourcing	1				1			
privacy	2	1						1
training & awareness	3	1	1					1
user participation	1		1					
vulnerability management	1				1			
Totals	**23**	**3**	**7**	**2**	**3**	**3**	**2**	**3**

Given that the nature of the firm is to minimize transaction costs (Coase, 1937), financial savings associated with IT outsourcing and IT offshoring should be carefully weighed against the cost of implementing the computer security controls necessary to offset the addition of IT outsourcing risk and IT offshoring risk. Increased computer security risk associated with host-country politics, delegation of administrative rights to foreign nationals, communication barriers, and cultural differences may offset any cost savings associated with perceived financial benefits (Gupta & Zhdanov, 2012; Hahn, Doh, & Bunyaratavej, 2009).

The consumption of IT is built upon a global digital infrastructure manifested by an interconnected mesh of computers, mobile devices, network connectivity, and application platforms. In turn, this global digital infrastructure has led to the emergence of new technologies such as cloud computing, social media, big data, smart phones, wearable technology, and 3D printing. Labeled variously as the Internet of Things, the industrial Internet of Things, or simply embedded systems, additional computer security controls are needed to mitigate the vulnerabilities exposed by new computer threats as organizations adopt emerging IT and digitally transform their global presence (Fichman, Dos Santos, & Zheng, 2014; Mithas, Ramasubbu, & Sambamurthy, 2011; Ransbotham, Mitra, & Ramsey, 2012).

Data classification and data privacy play an important role in enterprise computer security. The process required to identify and classify data according to a defined data sensitivity taxonomy is a precedent activity to implementing data privacy and data protection controls, as authorization, access and accountability controls can only be effective if the data to be protected is first accurately identified. Compounding the issue of data classification and data privacy is the myriad combination of state, federal, and international laws which define data privacy in different ways. The need to keep information private, along with the flexibility of sharing information when needed, also requires effective identity and access management controls. In addition to the financial cost of implementing effective controls, there may also be data processing performance costs resulting from latency issues associated with agent software, access table lookups, and data decryption routines. The exfiltration of more than 21 million sensitive, Office of Personnel Management (OPM) documents in June 2015 is but one example of the need for effective data

classification and privacy controls (Culnan & Williams, 2009; Gordon, Loeb, & Sohail, 2010; Vance, Lowry, & Eggett, 2015).

Enterprise computer security programs must also satisfy the requirements established for regulatory and industry compliance. Security controls for regulatory compliance with Sarbanes-Oxley (SOX) for financial reporting, Gramm-Leach-Bliley (GLBA) for financial data privacy, Health Insurance Portability and Accountability Act (HIPAA) for privacy of Protected Health Information (PHI) data, and privacy of Personally Identifiable Information (PII) data, must be incorporated into the enterprise computer security program. Industry compliance with Payment Card Industry (PCI) controls for credit card transactions is crucial for maintaining cash flow, given increasing reliance on electronic forms of payment. Another form of compliance is the top-down organizational recognition of enterprise computer security in the form of an organizational computer security policy. Workforce adherence to an organization wide computer security policy, supported by senior management, is an effective way to initiate a comprehensive computer security program across the enterprise. The decision by the Third U.S. Circuit Court of Appeals in August 2015 granting the Federal Trade Commission (FTC) the authority to investigate computer security incidents and potentially charge an offending organization with unfair trade practices for failure to properly secure sensitive data, serves notice of the need for due care and due diligence of computer security at the enterprise level (Bulgurcu et al., 2010; Li, Peters, Richardson, & Weidenmier Watson, 2012; Park, Sharman, & Rao, 2015; Puhakainen & Siponen, 2010; Siponen & Vance, 2010; S. Smith, Winchester, Bunker, & Jamieson, 2010; Spears & Barki, 2010; Vance et al., 2015).

Table 7. Number of Articles Published by MISQ, by Year, by Issue, Compared to Relevant Research Articles

Vol 33 Iss 1 thru Vol 39 Iss 2	Totals	2009	2010	2011	2012	2013	2014	2015
March	99	14	10	13	18	16	15	13
June	96	10	11	13	15	21	14	12
September	87	12	11	15	19	15	15	
December	88	12	11	15	18	17	15	
Totals	**370**	**48**	**43**	**56**	**70**	**69**	**59**	**25**
relevant research articles	23	3	7	2	3	3	2	3
Percent of Total	**6.22%**	**6.25%**	**16.28%**	**3.57%**	**4.29%**	**4.35%**	**3.39%**	**12.00%**

The implementation of computer security controls should follow a top-down, enterprise wide, master design that recognizes and incorporates discrete computing domains such as management information systems (IT security) and operational technology (OT security), with interlocking layers of security tools to provide a defense-in-depth solution built upon the security triad of confidentiality, integrity, and availability (CIA). Incorporating a top-down approach emphasizes the conscious recognition and understanding of the value provided by a holistically designed, enterprise computer security program (Chen, Kataria, & Krishnan, 2011; Juhee & Johnson, 2014; Li et al., 2012; S. Smith et al., 2010; Williams & Karahanna, 2013).

5. Research Gaps

The notion of a comprehensive approach to enterprise computer security is practical. Developing a holistic understanding of computer security from an enterprise perspective requires access to descriptive research that increases theoretical knowledge, as well as prescriptive research that increases practitioner productivity. Descriptive research and prescriptive research work together to inform each other. Descriptive research leads to theoretical findings that point to artifacts needed by practitioners, while prescriptive research creates useful artifacts that can be studied by behavioral researchers to learn more about how human behavior derives utility from each artifact (Goes, 2014; Gregor & Hevner, 2013). The relevant research articles selected for this literature review provide an overview of the extant research that is representative of enterprise computer security, but also point to research gaps needed for synthesis of a more comprehensive understanding.

For example, *what is senior management's perception of enterprise computer security?* Senior management must fully grasp and understand the issues associated with enterprise computer security in order to effectively build and sustain an enterprise culture of computer security. As with any enterprise objective, building a culture of computer security starts at the top and unless senior management supports such an effort the result will be less than adequate. Building a culture of computer security often starts with the creation of a new enterprise policy, which may require board approval.

Following agreement by senior management to enact a policy of enterprise computer security, *how does senior management decide upon the desired level of computer security, or risk threshold, they wish to impose across the enterprise?* While senior management might say that the objective of computer security is to prevent a single data breach from occurring, the practical response to that message will be a computer security program that is so restrictive that it brings organizational processes to a crawl and decreases the competitive ability of the organization. Likewise, a message that computer security should be loose enough to allow business to operate at the speed of thought might result in a computer security program that provides a false sense of security with no real protection from evolving computer threats. Senior management must have a solid understanding of the vulnerabilities exposed through the consumption of IT and the solutions that are practical, before they can decide upon the risk threshold that should be adopted for an enterprise computer security program.

Given the decision to achieve a desired level of computer security, *how does senior management communicate a risk threshold to IT?* Human communication is known to be vague and uncertain, and it is unlikely that a request for a conservative risk threshold will translate into the level of computer security desired by senior management. Failure to accurately communicate what is desired will result in the failure of IT to meet expectations, along with loss of trust between IT and senior management.

Once a risk threshold has been communicated from senior management to IT, *how does the IT organization transform a risk threshold into an interlocking set of computer security controls known as a defense-in-depth model?* Practitioner frameworks for computer security control models are readily available for consideration, but the process of translating a risk threshold into an operating set of controls that produces the desired level of computer security remains more a work of art than a work of science (ISACA, 2014; ISO, 2015; NIST SP-800 Computer Security, 2014). Advances in understanding how to translate a desired risk threshold into a functioning instantiation of a security controls framework requires additional research.

Given that humans represent the weakest link in computer security, *what can be done to reduce the risk of human vulnerability within computer security?* Aside from constant exposure to training and awareness programs, there are few defenses capable of protecting the organization from threats such as phishing emails or the inappropriate use of a USB flash drive. It matters not that a sophisticated defense-in-depth model blocks the vast majority of cybersecurity threats, if a single phishing email is able to successfully penetrate the network perimeter and deliver a malicious payload. The net effect to the organization is the same under either scenario; loss of IT prowess. Security tools are not perfect, and it is absurd to think that any security program will block every threat that it is designed to prevent. The concepts of bounded rationality and satisficing decision making underscore the need to better understand and manage the human aspect of computer security (Simon, 1996).

Lastly, *how does the IT organization communicate performance of a defense-in-depth computer security model to senior management, using terminology and symbolic language that senior management understands?* The packaging of technical information into a message devoid of technobabble that provides senior management with the information needed to ascertain whether or not a risk threshold is being met, and whether or not adjustments are necessary, is not as easy as it sounds. The ability to effectively communicate a comparison of computer security program performance against the financial investment required to build and maintain that program, is critical for building and maintaining trust between senior management and IT.

6. Limitations and Conclusions

This article provides a starting point to increase research about enterprise computer security. The methodology used to identify gaps has limitations. One major limitation is the decision to restrict this literature review to a single information systems research journal and a specific publication time frame. This was done in order to quickly gauge the academic work product that represents computer security from a comprehensive enterprise perspective. While this decision resulted in one perspective on the need for more research, a broader study involving additional journals might produce different results. For this reason, the methodology used by this study was described in detail so that others might benefit by repeating this methodology in similar, future studies.

A second limitation is the subjectiveness associated with the decision criterion used to select the relevant research articles for this study. Repeating this study using a similar methodology might produce different results, given the subjectiveness behind what actually constitutes computer security from an enterprise perspective.

A third limitation is that the categorization of relevant research articles might also be viewed as being subject to interpretation. Differences of interpretation are to be expected, and differences of opinion might serve as a basis for future research. Lastly, some might consider the reference section of this manuscript to be long relative to the length of the article. Given that this article constitutes a literature review, care was taken to intentionally include the references that contributed to the development of this article. In addition to providing transparency of content development, the reference section provides a solid resource for readers interested in learning more about enterprise computer security.

Enterprise computer security is an important topic for academic research given the rapid evolution of computer threats, and the need for organizations to better understand the collective vulnerabilities that enable computer security risk. While an initial keyword search for academic research related to enterprise computer security suggested that more than one-third of the articles published by MISQ from March 2009 through June 2015 involved some form of computer security from a comprehensive enterprise perspective, subsequent review of the search results followed by content analysis confirmed that academic research associated with a comprehensive understanding of computer security from an enterprise perspective is somewhat limited. In actuality, computer security research from a comprehensive enterprise perspective was found in only 6.22% of the 370 total MISQ articles reviewed. This finding suggests that enterprise computer security is an under studied research topic, and that meaningful opportunities for new descriptive and prescriptive research exist in this domain.

Of particular interest is research that contributes to the comprehensive understanding and management of enterprise computer security (Goes, 2014; Gregor & Hevner, 2013; Jansen, 2009; Lee, 2015; Straub & Welke, 1998).

Lastly, research opportunities also exist in the form of extending this literature review to the other journals in the AIS Senior Scholars' Basket of Journals (Table 1), and to other academic research journals that publish enterprise computer security research. Extending this literature review will help systematize and organize this field of research.

Acknowledgements

The author thanks the three anonymous reviewers, the managing editor, and the editor-in-chief for their constructive comments which helped to improve this paper.

References

Anonymous. (2010). War in the Fifth Domain; Cyberwar. *The Economist*, *396*, 25-28.

Association for Information Systems. (2015). Senior Scholars' Basket of Journals. Retrieved from http://ais.site-ym.com/?SeniorScholarBasket

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). INFORMATION SECURITY POLICY COMPLIANCE: AN EMPIRICAL STUDY OF RATIONALITY-BASED BELIEFS AND INFORMATION SECURITY AWARENESS. *MIS Quarterly*, *34*(3), 523-A527.

Carr, N. G. (2003). IT doesn't matter. *Harvard Business Review*, *81*(5), 41.

Carr, N. G. (2004). *Does IT Matter? Information Technology and the Corrosion of Competitive Advantage*. Boston, MA: Harvard Business School Press.

Carr, N. G. (2005). The End of Corporate Computing. *MIT Sloan Management Review*, *46*(3), 67-73.

Chen, P.-y., Kataria, G., & Krishnan, R. (2011). CORRELATED FAILURES, DIVERSIFICATION, AND INFORMATION SECURITY RISK MANAGEMENT. *MIS Quarterly*, *35*(2), 397-A393.

Coase, R. H. (1937). The Nature of the Firm. *Economica*, *4*(16).

Cole, D. (2014). The Three Leakers and What to Do About Them. *The New York Review of Books.* February 6, 2014. Retrieved from http://www.nybooks.com/articles/archives/2014/feb/06/three-leakers-and-what-do-about-them/

Culnan, M. J., & Williams, C. C. (2009). HOW ETHICS CAN ENHANCE ORGANIZATIONAL PRIVACY: LESSONS FROM THE CHOICEPOINT AND TJX DATA BREACHES. *MIS Quarterly*, *33*(4), 673-687.

Da Veiga, A., & Eloff, J. H. P. (2007). An information security governance framework. *Information Systems Management*, *24*(4), 361-372.

Dey, D., Lahiri, A., & Guoying, Z. (2014). QUALITY COMPETITION AND MARKET SEGMENTATION IN THE SECURITY SOFTWARE MARKET. *MIS Quarterly*, *38*(2), 589-A587.

Fichman, R. G., Dos Santos, B. L., & Zheng, Z. (2014). DIGITAL INNOVATION AS A FUNDAMENTAL AND POWERFUL CONCEPT IN THE INFORMATION SYSTEMS CURRICULUM. *MIS Quarterly*, *38*(2), 329-A315.

Gerber, M., & von Solms, R. (2001). From Risk Analysis to Security Requirements. *Computers & Security*, *20*(7), 577-584.

Gerber, M., & von Solms, R. (2005). Management of risk in the information age. *Computers & Security*, *24*(1), 16-30.

Gerber, M., & von Solms, R. (2008). Information security requirements – Interpreting the legal aspects. *Computers & Security*, *27*(5–6), 124-135.

Goes, P. B. (2014). Design Science Research in Top Information Systems Journals. *MIS Quarterly*, *38*(1), iii-viii.

Goldstein, J., Chernobai, A., & Benaroch, M. (2011). An Event Study Analysis of the Economic Impact of IT Operational Risk and its Subcategories. *Journal of the Association for Information Systems*, *12*(9), 606-631.

Gordon, L. A., Loeb, M. P., & Sohail, T. (2010). MARKET VALUE OF VOLUNTARY DISCLOSURES CONCERNING INFORMATION SECURITY. *MIS Quarterly*, *34*(3), 567-A562.

Greenberg, A. (2015). After Jeep hack, Chrysler recalls 1.4M vehicles for bug fix. *Wired.* Retrieved from http://www.wired.com/2015/07/jeep-hack-chrysler-recalls-1-4m-vehicles-bug-fix/

Gregor, S., & Hevner, A. R. (2013). POSITIONING AND PRESENTING DESIGN SCIENCE RESEARCH FOR MAXIMUM IMPACT. *MIS Quarterly*, *37*(2), 337-355.

Gupta, A., & Zhdanov, D. (2012). GROWTH AND SUSTAINABILITY OF MANAGED SECURITY SERVICES NETWORKS: AN ECONOMIC PERSPECTIVE. *MIS Quarterly*, *36*(4), 1109-A1107.

Hahn, E. D., Doh, J. P., & Bunyaratavej, K. (2009). THE EVOLUTION OF RISK IN INFORMATION SYSTEMS OFFSHORING: THE IMPACT OF HOME COUNTRY RISK, FIRM LEARNING, AND COMPETITIVE DYNAMICS. *MIS Quarterly*, *33*(3), 597-616.

ISACA. (2014). Information Systems Audit and Control Association. Retrieved from www.isaca.org

ISO. (2015). ISO/IEC 27001 - Information security management. Retrieved from http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

Jansen, W. (2009). *NISTIR 7564 Directions in Security Metrics Research*. National Institute of Standards and Technology.

Johnston, A. C., & Warkentin, M. (2010). FEAR APPEALS AND INFORMATION SECURITY BEHAVIORS: AN EMPIRICAL STUDY. *MIS Quarterly, 34*(3), 549-A544.

Johnston, A. C., Warkentin, M., & Siponen, M. (2015). AN ENHANCED FEAR APPEAL RHETORICAL FRAMEWORK: LEVERAGING THREATS TO THE HUMAN ASSET THROUGH SANCTIONING RHETORIC. *MIS Quarterly, 39*(1), 113-A117.

Juhee, K., & Johnson, M. E. (2014). PROACTIVE VERSUS REACTIVE SECURITY INVESTMENTS IN THE HEALTHCARE SECTOR. *MIS Quarterly, 38*(2), 451-A453.

Lee, J. K. (2015, 06//). GUEST EDITORIAL: Research Framework for AIS Grand Vision of the Bright ICT Initiative, Editorial. *MIS Quarterly*, pp. iii-xii.

Li, C., Peters, G. F., Richardson, V. J., & Weidenmier Watson, M. (2012). THE CONSEQUENCES OF INFORMATION TECHNOLOGY CONTROL WEAKNESSES ON MANAGEMENT INFORMATION SYSTEMS: THE CASE OF SARBANES-OXLEY INTERNAL CONTROL REPORTS. *MIS Quarterly, 36*(1), 179-204.

Liang, H., & Xue, Y. (2009). AVOIDANCE OF INFORMATION TECHNOLOGY THREATS: A THEORETICAL PERSPECTIVE. *MIS Quarterly, 33*(1), 71-90.

Mata, F. J., Fuerst, W. L., & Barney, J. B. (1995). Information Technology and Sustained Competitive Advantage: A Resource-Based Analysis. *MIS Quarterly, 19*(4), 487-505.

McFadzean, E., Ezingeard, J. N., & Birchall, D. (2007). Perception of risk and the strategic impact of existing IT on information security strategy at board level. *Online Information Review, 31*(5), 622-660.

Merhout, J. W., & O'Toole, J. (2015a). Enhancing the Control Objectives for Information and Related Technologies (COBIT 5) Framework for Sustainable IT Governance. *Journal of the Midwest Association for Information Systems, 2015*(2).

Merhout, J. W., & O'Toole, J. (2015b). *Sustainable IT Governance (SITG): Is COBIT 5 An Adequate Model?* Paper presented at the Proceedings of the Tenth Midwest Association for Information Systems Conference, Pittsburg State University, Pittsburg, KS.

MIS Quarterly. (2015). About MIS Quarterly. Retrieved from www.misq.org

Mithas, S., Ramasubbu, N., & Sambamurthy, V. (2011). HOW INFORMATION MANAGEMENT CAPABILITY INFLUENCES FIRM PERFORMANCE. *MIS Quarterly, 35*(1), 237-256.

National Intelligence Council. (2008). *Disruptive Civil Technologies - Six Technologies with Potential Impacts on US Interests out to 2025*.

NIST SP-800 Computer Security. (2014). National Institute of Standards and Technology Computer Security Resource Center. *Special Publications (800 Series).* Retrieved from http://csrc.nist.gov/publications/PubsSPs.html

Park, I., Sharman, R., & Rao, H. R. (2015). DISASTER EXPERIENCE AND HOSPITAL INFORMATION SYSTEMS: AN EXAMINATION OF PERCEIVED INFORMATION ASSURANCE, RISK, RESILIENCE, AND HIS USEFULNESS. *MIS Quarterly, 39*(2), 317-A319.

Ponemon Institute. (2015). 2015 Global Megatrends in Cybersecurity. Retrieved from http://www.raytheon.com/news/rtnwcm/groups/gallery/documents/content/rtn_233811.pdf

Porter, M. E. (1979). How competitive forces shape strategy. *Harvard Business Review, 57*(2), 137-145.

Porter, M. E. (1980). *Competitive Strategy. Techniques for Analyzing Industries and Competitors*. New York, NY: The Free Press.

Porter, M. E. (1985). *Competitive Advantage. Creating and Sustaining Superior Performance.* New York, NY: The Free Press.

Posey, C., Roberts, T. L., Lowry, P. B., Bennett, R. J., & Courtney, J. F. (2013). INSIDERS' PROTECTION OF ORGANIZATIONAL INFORMATION ASSETS: DEVELOPMENT OF A SYSTEMATICS-BASED TAXONOMY AND THEORY OF DIVERSITY FOR PROTECTION-MOTIVATED BEHAVIORS. *MIS Quarterly, 37*(4), 1189-A1189.

Posthumus, S., & von Solms, R. (2004). A framework for the governance of information security. *Computers & Security, 23*(8), 638-646.

Privacy Rights Clearinghouse. (2015). Data Breach Chronology. Retrieved from http://www.privacyrights.org/data-breach

Puhakainen, P., & Siponen, M. (2010). IMPROVING EMPLOYEES' COMPLIANCE THROUGH INFORMATION SYSTEMS SECURITY TRAINING: AN ACTION RESEARCH STUDY. *MIS Quarterly, 34*(4), 767-A764.

PwC. (2015). US cybersecurity: Progress stalled Key findings from the 2015 US State of Cybercrime Survey. Retrieved from http://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/2015-us-cybercrime-survey.pdf

Rai, A., Pavlou, P. A., Im, G., & Du, S. (2012). INTERFIRM IT CAPABILITY PROFILES AND COMMUNICATIONS FOR COCREATING RELATIONAL VALUE: EVIDENCE FROM THE LOGISTICS INDUSTRY. *MIS Quarterly*, *36*(1), 233-A235.

Ransbotham, S., Mitra, S., & Ramsey, J. (2012). ARE MARKETS FOR VULNERABILITIES EFFECTIVE? *MIS Quarterly*, *36*(1), 43-64.

Simon, H. (1996). *The Sciences of the Artificial* (3rd ed.). Cambridge, MA: MIT Press.

Siponen, M., & Vance, A. (2010). NEUTRALIZATION: NEW INSIGHTS INTO THE PROBLEM OF EMPLOYEE INFORMATION SYSTEMS SECURITY POLICY VIOLATIONS. *MIS Quarterly*, *34*(3), 487-A412.

Smith, H. A., & McKeen, J. D. (2009). Developments in Practice XXXIII: A Holistic Approach to Managing IT-based Risk. *Communications of the Association for Information Systems*, *25*, 519-530.

Smith, S., Winchester, D., Bunker, D., & Jamieson, R. (2010). CIRCUITS OF POWER: A STUDY OF MANDATED COMPLIANCE TO AN INFORMATION SYSTEMS SECURITY DE JURE STANDARD IN A GOVERNMENT ORGANIZATION. *MIS Quarterly*, *34*(3), 463-486.

Spears, J. L., & Barki, H. (2010). USER PARTICIPATION IN INFORMATION SYSTEMS SECURITY RISK MANAGEMENT. *MIS Quarterly*, *34*(3), 503-A505.

Straub, D. W., & Welke, R. J. (1998). Coping With Systems Risk: Security Planning Models for Management Decision Making. *MIS Quarterly*, *22*(4), 441-469.

U.S. Army Cyber Command. (2015). Establishment of U.S. Army Cyber Command. Retrieved from http://www.arcyber.army.mil/history_arcyber.html

Van Niekerk, J. F., & Von Solms, R. (2010). Information security culture: A management perspective. *Computers & Security*, *29*(4), 476-486.

Vance, A., Lowry, P. B., & Eggett, D. (2015). INCREASING ACCOUNTABILITY THROUGH USER-INTERFACE DESIGN ARTIFACTS: A NEW APPROACH TO ADDRESSING THE PROBLEM OF ACCESS-POLICY VIOLATIONS. *MIS Quarterly*, *39*(2), 345-A348.

Verizon. (2015). Verizon Data Breach Investigations Reports. Retrieved from http://www.verizonenterprise.com/DBIR/

Vijayan, J. (2009). Defense Secretary Gates approves creation of U.S. Cyber Command. Retrieved from http://www.computerworld.com/article/2525896/cybercrime-hacking/defense-secretary-gates-approves-creation-of-u-s--cyber-command.html

von Solms, B. (2001a). Corporate Governance and Information Security. *Computers & Security*, *20*(3), 215-218.

von Solms, B. (2001b). Information Security - A Multidimensional Discipline. *Computers & Security*, *20*(6), 504-508.

von Solms, B., & von Solms, R. (2005). From information security to…business security? *Computers & Security*, *24*(4), 271-273.

von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97-102.

von Solms, R., & von Solms, S. H. (2006). Information security governance: Due care. *Computers & Security*, *25*(7), 494-497.

Westerman, G., & Hunter, R. (2007). *IT Risk: Turning Business Threats into Competitive Advantage*. Boston, Massachusetts: Harvard Business School Press.

Williams, C. K., & Karahanna, E. (2013). CAUSAL EXPLANATION IN THE COORDINATING PROCESS: A CRITICAL REALIST CASE STUDY OF FEDERATED IT GOVERNANCE STRUCTURES. *MIS Quarterly*, *37*, 933-A938.

Willison, R., & Warkentin, M. (2013). BEYOND DETERRENCE: AN EXPANDED VIEW OF EMPLOYEE COMPUTER ABUSE. *MIS Quarterly*, *37*(1), 1-20.

Zetter, K. (2011). How digital detectives deciphered Stuxnet, the most menacing malware in history. *Wired.* Retrieved from http://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/

Zetter, K. (2015). A cyberattack has caused confirmed physical damage for the second time ever. *Wired.* Retrieved

from http://www.wired.com/2015/01/german-steel-mill-hack-destruction/

Zuccato, A. (2004). Holistic security requirement engineering for electronic commerce. *Computers & Security*, *23*(1), 63-76.

Zuccato, A. (2007). Holistic security management framework applied in electronic commerce. *Computers & Security*, *26*(3), 256-265.

Author Biography

Dennis Acuña (dcacuna@dsu.edu) is an IT practitioner in the oil and gas industry. He has held technical and supervisory positions of increasing responsibility in systems analysis & programming, database management, telecommunications, operations research, and computer security & compliance. Acuña earned his BBA and MBA degrees from the University of Toledo and his M.Sc. from Bowling Green State University. He is a member of ISACA (CISM, CRISC), and is currently working toward completion of his doctorate degree (D.Sc. IS) from Dakota State University.