Presented to the Interdisciplinary Studies Program:

UNIVERSITY OF OREGON
APPLIED INFORMATION MANAGEMENT

Applied Information Management and the Graduate School of the University of Oregon in partial fulfillment of the requirement for the degree of Master of Science

Information Security Culture: Fusion of Professional and Personal Lives

CAPSTONE REPORT

Dennis Copas Jr.
Technology Infrastructure Manager
OnPoint Community Credit Union

University of Oregon
Applied Information Management
Program

May 2015

Academic Extension
1277 University of Oregon
Eugene, OR 97403-1277
(800) 824-2714

Approved by

Dr. Kara McFall
Lecturer, AIM Program

Information Security Culture: Fusion of Professional and Personal Lives

Dennis Copas Jr.

OnPoint Community Credit Union

Abstract

This annotated bibliography explores the core values organizations must possess in order to implement information security cultures that incorporate information security awareness and develop information security behaviors while maximizing productivity and reducing the number of security incidents created from end users. The bibliography is based on literature published from 2005 to 2015. Conclusions drawn from the literature describe the different corporate culture frameworks and training methodologies needed to cultivate an information security culture.

Keywords: corporate culture, data breaches, information security, security awareness, security behavior and security training.

Table of Contents

Introduction

Problem Statement

Information Technology security breaches and identity thefts have appeared prominently in the headlines of major newspapers and magazines. The number of incidents continues to grow at a staggering rate, with over 700 data breaches taking place in 2014, which was an increase of 26% from 2013 (Smith, 2015). Common IT security threats include (a) stealing confidential information, (b) Denial of Service attacks, (c) extortion, and (d) malware, which is software that is created to perform malicious actions like identity theft (SANS, 2014). There are many different types of malware. The more commonly known types of malware are viruses and bot nets. Viruses have the ability to copy themselves into other programs (Hardikar, 2008), while bot nets, or bots as they are more commonly referred to rely on a command and control system, which provides instructions to bots to gather and send information back to the control server (Hardikar, 2008).

With the growing popularity of such technologies as Software- and Infrastructure-as-a-Service and mobile computing, new behaviors for end users have emerged that enable security breaches. These behaviors include using public wireless access points for access to the Internet and staying constantly connected to the Internet; devices are rarely powered off or disconnected from the Internet. As a result of these new behaviors, new security breaches have emerged, including (a) Man-in-the-Middle attacks when an intruder becomes a relay between two systems, (b) Distributed Denial of Service attacks that overload systems with data until the systems shut down or become unresponsive; and (c) SQL injections when a client injects SQL commands to disrupt service to databases (Grobauer, Walloschek, & Stocker, 2011). Other threats to IT security that exploit new user behaviors include mobile malware from Bring-Your-Own Device environments and cloud applications that do not utilize strong encryption (Schiff, 2015); both the behaviors and ensuing threats create new challenges for information security departments. These challenges include inadvertent or intentional acts resulting in security breaches by insiders, malware from third party vendors, and zero-day event, which is malware that does not have an established fix (Fischer, 2014). To add to the challenges introduced from new technologies, more sophisticated threats continue to emerge, increasing the potential for data breaches. Examples include DyreWolf and Heartbleed, which are sophisticated threats that leverage system vulnerabilities and social engineering to bypass security appliances, thus allowing the hacker to gain a foothold in the organization (Lennon 2015).

The costs of IT security breaches are high. According to Caldwell (2014), an information security breach will cost an organization on average $917,884. The estimated cost includes forensics research, legal costs, public communication, and the building or expanding of call centers to handle the ensuing customer service calls that result from the theft of customer data (IBM, 2014). Many organizations struggle with data breaches. According to IBM (2014), only 32 percent of organizations are able to manage and respond to data breaches (IBM, 2014). Organizations need to understand their current information security programs and prepare for future technology that will address new and existing security concerns.

In many organizations, end users are viewed as the “weakest link” in information security management (Ken, Yuan, Archer, & Connelly, 2011), making the end user a security liability. While most end user actions are non-malicious and unintentional, the end users’ actions still create an information security gap for organizations (Ken et al., 2011). The Online Trust Alliance (2015) stated in 2014 that 29 percent of data breaches were a result of employee actions, either accidental or intentional. On average it would have cost organizations in 2014 about $3.5 million to recover from these breaches, which was an increase of 15 percent from 2013 (IBM, 2014). With environments that change continuously, one approach that organizations can take to address the shifting security landscape is to implement information security strategies that establish information security cultures (Van Niekerk & Von Solms, 2009).

Creating an information security culture is a commitment from organizations to their employees and patrons. Organizations need commitments from end users to develop and incorporate information security behavioral patterns into their professional and personal lives (Parsons, McCormac, Butavicius, Pattinson, & Jerram, 2013). Individuals who adopt information security behaviors in their personal lives will develop increased threat perceptions, evaluate safeguard measures, and engage in threat avoidance behavior (Huigang, & Yajiong, 2010). The heightened level of vigilance benefits the individual's place of employment because these security practices prevent or limit security incidents at the workplace.

Many organizations recognize the need to develop information security cultures, but there are other competing organizational priorities (Johnson & Goetz, 2007). Development of the information security culture requires that the new culture does not interfere with business goals while having minimal costs (Van Niekerk & Von Solms, 2009). Security is paramount, but not to the levels that impede the organization's ability to grow (Johnson & Goetz, 2007).

Purpose of the Study

The purpose of this study is to identify research sources that describe how IT security managers can develop security processes that individual employees can adopt in their personal lives that will carry over into their professional lives. Shaw, Chen, Harris, and Huang, (2009) define security culture as the understanding of users about the importance of information security and their responsibilities and acts to exercise sufficient levels of information security control to protect the organization's data and networks. Research sources are included that describe the different types of security breaches, the costs of these breaches, and efforts to date to address them (Krausz & Walker, 2013). Specific emphasis is applied to sources that describe security breaches that are intentionally or unintentionally caused by user behavior, as well as changing user behaviors that exacerbate the risks (Mitra & Ransbotham, 2009). The focus of this study is to identify research to inform the development of an information security culture framework for small to medium organizations (10-500 employees) using a case study method of inquiry, along with incorporating grounded theory approaches. Sources are also sought that describe measurable tools as part of the information security framework, to monitor the adoption and progress of an information security culture.

Research Question

Main question. In the contexts of human behavior, corporate culture and information security, how can organizations implement a security culture while maximizing productivity?

Sub-question. What values must an organization possess for end users to adopt information security cultures?

Audience

The audience for this annotated bibliography includes Information Security professionals, Information Technology Managers, Training and Development Managers, and Executives in medium to large organizations. These key individuals and groups are responsible for the implementation and adoption of an information security culture (Parsons, McCormac, Butavicius, Pattinson & Jerram, 2013). Information Security professionals are obvious stakeholders, as they both influence information security practices and are called upon to respond to breaches in security (Fischer, 2014). Information Technology Managers have a vested interest in information security because they reduce risk by reviewing and implementing information security policies, along with ensuring team members have the correct skill sets needed to prevent security incidents (National Institute of Standards and Technology, 2010). Organizational executives and senior leaders are responsible for establishing and promoting the culture of an organization (Da Veiga & Martins, 2015), and thus will have a large impact on the success or failure of information security cultures in their own organizations. For an information security culture to be successful in an organization it must (a) maximize productivity, (b) result in a minimal financial burden, and (c) be linked to current business strategies (Johnson & Goetz, 2007).

Search Report

Search strategy. The University of Oregon Library provides the ability to locate information pertaining to Information Security Culture with minimal effort. The initial search provides over 110 articles spanning almost 20 years. To refine the research the subject is divided into three categories. These categories are *corporate culture, information security* and *corporate governance* (Thompson & Solms, 2005). The following keywords yield the research sources: *corporate culture, data breaches, information security, security awareness*, *security behavior* and *security training*. With the speed with which technology is evolving, the date range for publication dates ranges from 2005 to 2015, with a focus on information from 2010 or later to ensure the most current information. In an effort to refine the search even more, sources produced by military, national organizations and governments are also removed. The resulting research resources are a combination of journal articles and scholarly studies that use qualitative and quantitative research methods.

Establish index descriptors. Information security culture is a social culture that incorporates technical security measures (Ruighaver, Maynard, Chang, & Maynard, 2007). Ruighaver et al. (2007) believe implementing an information security framework will greatly influence individuals and groups towards improved information security behaviors. A successful information security framework has three major components: corporate governance, information security and corporate culture (Thompson & Solms, 2005). Each of these components has their own descriptions. According to the Organization for Economic Cooperation and Development (2004), corporate governance is a set of relationships between a company's management, its board and its stakeholders that provides structure for the company and the mechanism to set objectives. Information security is the protection of information systems against unauthorized access or modification of information (National Security Telecommunications and Information Systems Security Committee, 2000). According to *Dictionary.com* (2015), corporate culture is defined as the philosophy, values and policies of a company. The common keywords by authors for these three categories include:

- Corporate culture
- Corporate governance
- Data breaches
- Groups
- Information security
- Motivation
- Organization culture
- Security awareness
- Security behaviors

- Training
- Users

Search engines and databases. Utilizing key terms and different search options within the databases for Academic Search Premier, Cambridge Journal, EBSCO, JSTOR, UO Local Catalog and the Wiley Online Library produces a number of relevant articles, listed in the Annotated Bibliography.

Document Approach

For this scholarly annotated bibliography full text articles relating to information security culture has been selected, reviewed and downloaded from UO Library, databases, and different search engines. Management of documents is a manual process in which a Microsoft Word document is used to create a master list containing the following information: (a) *authors' names,* (b) *dates of publications,* (c) *titles of the documents*, (d) *locations where the documents can be retrieved*, and (e) *article abstract*. The references gathered for the study are divided into four categories: (a) *Corporate culture*, (b) *End-user IT security behavior*, (c) *Information Security Management* and (d) *Training methods.* All articles are in portable document format (PDF), cited and stored in the same on the personal computer's local drive and on an external drive. A backup is created daily to ensure the data is protected.

Reference Evaluation Criteria

The references for this annotated bibliography are evaluated using criteria established by Bell and Frantz (2014). The following evaluation criteria are: (a) authority, (b) objectivity, (c) quality, (d) currency, and (e) relevancy.

Authority. As suggested by Bell and Frantz (2014), authority addresses the author's credibility amongst his or her peers within the author's field, relevant or specialized work experience, and the author's affiliations such as universities or respected institutions. Authority also includes an author's credentials, such as advanced degrees or industry certifications. The authors cited in this annotated bibliographies are verified through the University of Oregon library and Google Scholar to ensure they meet Bell and Frantz's (2014) criteria for authority.

Objectivity. All articles are reviewed in an effort to identify the author's goal in writing the publication to make sure the intent is to inform rather than sell a product or service or advocate for an agenda; ensure the author's information is well-researched and supported by evidence; and to determine if the author exhibited any biases (Bell & Frantz, 2014).

Quality. Quality is identified and measured by the author's ability to create a logical structure by defining clear points and ensuring a logical flow of the content. The research sources are also validated for the use of good grammar and accurate statistical information and by the absence of typographical errors (Bell & Frantz, 2014).

Currency. As suggested by Bell and Frantz (2014), research on topics involving science should use sources that are most up to date. All articles used possess a publication date of 10 years or less to ensure the information is relevant to a technology world that is continuously evolving.

Relevancy. Articles that contain content that pertains to the keywords for this study are considered relevant. Reference material is selected from scholarly sources and consists primarily of secondary sources (Bell & Frantz, 2014).

Annotated Bibliography

The following Annotated Bibliography presents 15 references that provide a comprehensive overview of an information security culture, with an emphasis on sources that describe the importance of users to the success or failure of information security programs that are intended to protect an organization's data and networks (Shaw, Chen, Harris, & Huang, 2009). The references provide information security professionals, Information Technology Managers, and executives in medium to large organizations with the information and values required to adopt and implement information security cultures within their organizations (Thompson & Solms, 2005). References are presented in three categories: (a) information security culture, (b) end-user information security behavior, and (c) training methods.

Each annotation consists of three elements: (a) the formal bibliographic citation in APA format sixth edition; (b) the published abstract, which covers the main points; and (c) a summary of how the reference addresses the problem, the research question, and/or the audience of the study. The ideas presented in the summary are those of the author(s) of the original works and not the author of this annotated bibliography.

Information Security Culture

Ashenden, D. & **Sasse A.** (2013, November). CISOs and organizational culture: Their own worst enemy?. *Computers and Security*, *39*(B), 396-405. doi: 10.1016/j.cose.2013.09.004

Abstract. Many large organizations now have a Chief Information Security Officer (CISO[1]). While it may seem obvious that their role is to define and deliver organizational security goals, there has been little discussion on what makes a CISO able to deliver this effectively. In this paper, we report the results from 5 in-depth interviews with CISOs, which were analyzed using organizational behavior theory. The results show that the CISOs struggle to gain credibility within their organization due to: a perceived lack of power, confusion about their role identity, and their inability to engage effectively with employees. We conclude that as the CISO role continues to develop CISOs need to reflect on effective ways of achieving credibility in their organizations and, in particular, to work on communicating with employees and engaging them in security initiatives. We also identify a key responsibility for effective CISOs; that is to remove the blockages that prevent information security from becoming 'business as usual' rather than a specialist function. For researchers, our findings offer a new piece of the emerging picture of human factors in information security initiatives.

Summary. This article focuses on the Chief Information Security Officer's (CISO's) role within the organization and how the role is changing. CISOs are now being challenged with implementing security awareness programs. Ashenden and Sasse interviewed five CISOs using the qualitative method of research. The authors' data identified three circuits of discourse: (a) Circuit of Activity, the initial message communication; (b) Circuit of Performativity, when the new message is received or rejected; and (c) the Circuit of Connectivity, when the message is embedded in the organizational culture. The article identifies the challenge associated with the Circuit of Performativity because the CISO is viewed as being authoritarian, providing one-way communication through policies and directives. For CISOs to achieve the Circuit of Connectivity, CISOs must establish two-way communication with the employees and share the responsibilities for understanding security awareness.

Da Veiga, A., & Martins, N. (2015, March). Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers and Security*, *49*(3), 162-176 doi: 10.1016/j.cose.2014.12.006

Abstract. The human aspect, together with technology and process controls, needs to be considered as part of an information security program. Current and former employees are still regarded as one of the root causes of information security incidents. One way of addressing the human aspect is to embed an information security culture where the interaction of employees with information assets contributes to the protection of these assets. In other words, it is critical to improve the information security culture in organizations such that the behavior of employees is in compliance with information security and related information processing policies and regulatory requirements. Assessing, monitoring and influencing an information security culture can achieve this. An information security culture is assessed by using an approach such as an information security culture assessment (ISCA). The empirical data derived from an ISCA can be used to influence the information security culture by focusing on developmental areas, of which awareness and training programs is a critical facet.

In this paper we discuss a case study of an international financial institution at which ISCA was conducted at four intervals over a period of eight years, across twelve countries. Comparative and multivariate analyses were conducted to establish whether the information security culture improved from one assessment to the next based on the developmental actions implemented.

Summary. This article by Da Veiga and Martins supports the premise that if an information security culture is to be successful in an organization, it requires a

commitment from senior management. Implementing a security awareness program is one of the commitments. Da Veiga and Martins utilize the quantitative research method to gather data from 12 countries through questionnaires from an Information Security Culture Assessment tool. The authors' research supports the premise that by providing annual information security training to the organizations' employees, the employees' information security intelligent quotient (IQ) rose. As individual's information security IQ began to rise, so did the employees' information security behavior, thus improving the organization's information security culture. An annual assessment was conducted over a four-year span to measure how well the information security of the organizations surveyed improved over time. Each of the 12 countries did show improvement in information security within their respective organizations.

Johnson, M.E., & Goetz, E. (2007, June). Embedding information security into the organization. *Security & Privacy, IEEE , 5*(3), 16-24. doi:10.1109/MSP.2007.59

Abstract. Risk and business have always been inseparable, but new information security risks pose unknown challenges. How should firms organize and manage to improve enterprise security? Here, the authors describe how chief information security officer (CISOs) are working to build secure organizations.

Summary. The article focuses on how businesses need to incorporate an information security culture to assist with identifying different types of security risks such as strategic risk, financial risk, and operation risk within the organization. An information security culture will assist in the assessment and mitigation of the risks. The executives and senior management within the organization must communicate the need for an information security culture for the organization to the employees. This article addresses the problem

statement on the need for commitment from senior management in order to implement an information security culture. Businesses continue to grow and move forward, but during this growth process businesses have to stay conscious of information security. Businesses are facing many challenges related to regulations, globalization, and innovation, along with periods of both growth and recession. All of these challenges make it difficult for businesses to manage information security. This is why Johnson and Goetz recommend using analytics to monitor different metrics to measure how the organization's information security culture is being maintained. In an effort to secure the business, the Chief Information Security Officer needs to understand the business and align the security goals with the goals of the business.

Mitra, S., & Ransbotham, S., (2009). Choice and chance: a conceptual model of paths to information security compromise. *Information Systems Research, 20*(1), 121+. Retrieved from http://go.galegroup.com/ps/i.do?id=Gale%7CA197186605&v=2.1&u=s8492775&it=r&p=AONE&sw=w&asid=7c5793a220f2c60310fcb17048a2fe80

Abstract. No longer the exclusive domain of technology experts, information security is now a management issue. Through a grounded approach using interviews, observations, and secondary data, we advance a model of the information security compromise process from the perspective of the attacked organization. We distinguish between deliberate and opportunistic paths of compromise through the Internet, labeled choice and chance, and include the role of counter measures, the Internet presence of the firm, and the attractiveness of the firm for information security compromise. Further, using one year of alert data from intrusion detection devices, we find empirical support for the key contributions of the model. We discuss the implications of the model for the emerging research stream on information security in the information systems literature.

Summary. This article focuses on the creation of the information security compromised process (ISCP) model, which has two distinct paths (a) deliberate, and (b) opportunistic. The deliberate path is a targeted attack on an organization. Targeted attacks are usually made for information gain, financial gain, or to cause harm to an organization's reputation, while opportunistic attacks usually gain access through a misconfigured system or vulnerability that does not have a patch to address the vulnerability. The authors Mitra and Ransbortham were able to successfully create an ISCP model. The ISCP model also identifies reasons for attacks and attack patterns in hopes of creating countermeasures. The article provides examples of why hackers are attracted to different businesses and how members of information security teams and end users need to have the knowledge and skill sets to protect them from being possible victims. The needed foundational organizational values required to secure an information environment are for employees to embrace meticulous attention to security risks and be vigilant and guarded, which addresses the sub question of this research study of what values are needed by an organization to implement an information security culture.

Rastogi, R., & von Solms, R., (2012). Information security service culture - information security for end-users. *Journal of Universal Computer Science, 18*(12), 1628-1642.

Abstract. Information security culture has been found to have a profound influence on the compliance of end-users to information security policies and controls in their organization. Similarly, a complementary aspect of information security is the culture of information security managers and developers in the organization. This paper refers to this an “information security service culture’ (ISSC). ISSC shapes and guides the behaviour of information security managers and developers as they formulate information security policies and controls. Thus, ISSC has profound influence on the nature of these policies and controls and thereby on the interaction of end-users with these artifacts. ISSC is useful in transforming information security managers and developers from their present-day technology-focused approach to an end-user centric approach.

Summary. The paper examines how the Information Security Culture is expanding from information security awareness to the development of a service organization approach for information security managers and professionals. This concept is referred to as an Information Security Service Culture. Information security professionals are asked to gain a better understanding of the end users’ daily tasks and patterns in an effort to develop security policies that do not impede on the end users’ abilities to deliver services or solutions to fellow teammates or customers. According to the authors, the desire to understand the end users will improve communication and break down the *Us versus You* perception held by many end users towards information security professionals. The article also focuses on communication as the key to sharing information security beliefs and values, in which end users adopt the information security culture and become security assets. Additional research must be completed to support the premise that an Information Security Service Culture is needed to instill an information security culture in an organization.

Ruighaver, A., Chang, S. , & Maynard, S. (2007). Organisational security culture: Extending the end-user perspective. *Computers & Security*, *26*(1), 56-62.

Abstract. The concept of security culture is relatively new. It is often investigated in a simplistic manner focusing on end-users and on the technical aspects of security. Security, however, is a management problem and as a result, the investigation of security culture should also have a management focus. This paper describes a framework of eight dimensions of culture. Each dimension is discussed in terms of how they relate specifically to security culture based on a number of previously published case studies. We believe that use of this framework in security culture research will reduce the inherent biases of researchers who tend to focus on only technical aspects of culture from an end-users perspective.

Summary. This article focuses on how to implement an information security culture framework using established organizational frameworks. The challenges experienced when utilizing an organizational culture framework to implement an information security culture framework are evident when attempting to integrate information security components, such as creating and implementing restrictive polices impeding individuals from performing their jobs in an efficient manner. Using case studies, Ruighaver, Chang, and Maynard also discovered that employee motivation declines when there is a lack of communication with new security policies and accountability, making it harder to build or improve on a current information security culture. The authors believe the concept of an organization framework is a good starting point in implementing an information security culture framework. The authors recommend focusing on one or two important information security aspects for the organization as a beginning step to implementation.

Thomson, K., & von Solms, R. (2005). Information security obedience: A definition. *Computers & Security*, *24*(1), 69-75. doi:10.1016/j.cose.2004.10.005

Abstract. Information is a fundamental asset within any organisation and the protection of this asset, through a process of information security, is of equal importance. This paper examines the relationships that exist between the fields of corporate governance, information security and corporate culture. It highlights the role that senior management should play in cultivating an information security conscious culture in their organisation, for the benefit of the organisation, senior management and the users of information.

Summary. Information security obedience: The definition offered by the authors focuses on senior management's dedication to an information security culture. This article addresses the problem statement by identifying that commitment is one of the values needed in order to implement an information security culture. The article describes how an information security culture is achieved through three different attributes of the organization: (a) corporate governance, (b) corporate culture, and (c) information security. The authors identify the attribute of corporate governance as the bylaws and policies of an organization, while corporate culture is the beliefs and behaviors of the organization. The final attribute is information security. The goals when implementing information security policies are to identify all technology risks and apply security controls to mitigate the risks, so the organization can achieve the strategic goals set forth by senior management and the board. It is the responsibility of the board and senior management to incorporate information security into every one of their decisions. The actions mandated by the board and senior management are to protect and consciously manage data in a secure manner. The actions will be seen and heard and similarly executed by the end users. End users will begin adopting information security behavior, which will develop the information security culture, and information security behavior will become natural.

Van Niekerk, J. F. & Von Solms, R. (2009, June). Information security culture: A management perspective. *Computers and Security*, *29*(4), 476-486 doi: 10.1016/j.cose.2009.10.005

Abstract. Information technology has become an integral part of modern life. Today, the use of information permeates every aspect of both business and private lives. Most organizations need information systems to survive and prosper and thus need to be serious about protecting their information assets. Many of the processes needed to protect these information assets are, to a large extent, dependent on human cooperated behavior. Employees, whether intentionally or through negligence, often due to a lack of knowledge, are the greatest threat to information security. It has become widely accepted that the establishment of an organizational sub-culture of information security is key to managing the human factors involved in information security. This paper briefly examines the generic concept of corporate culture and then borrows from the management and economical sciences to present a conceptual model of information security culture. The presented model incorporates the concept of elasticity from the economical sciences in order to show how various variables in an information security culture influence each other. The purpose of the presented model is to facilitate conceptual thinking and argumentation about information security culture.

Summary. The article focuses on the idea that information drives businesses today and that businesses can no longer function without timely and relevant information. However, many businesses lack an information security culture, mainly because security is viewed as detrimental to the business. The authors utilized economic and managerial science to establish the conflicts of interest when attempting to implement an information security culture. These conflicts include unintentional non-compliance with information security policies, intentional negligence when attempting to commit a work task, the risks posed by greater access compared to restricted access, and the limitations of different access points or devices. Once all of the conflicts were identified, the authors then used a corporate culture framework to identify what values and attributes are needed to implement an information security culture. The attribute that an employee needs to possess is *espoused values,* which in the context of an information security culture is the employee's views toward information security. In addition, the organization needs to develop their *shared tacit assumptions*, which reflect the organization's willingness to adopt beliefs or behaviors. Through Van Niekerk and Von Solms' research, the authors identified another key attribute that is required by all organizations that want to implement an information security culture: knowledge. Employees need to have an understanding of information security to create the desire to learn and adopt information security as a culture.

End-user information security behavior

Ken H, G. , Yuan, Y. , Archer, N. , & Connelly, C. (2011). Understanding non-malicious security violations in the workplace: A composite behavior model. *Journal of Management Information Systems*, *28*(2), 203-236.

Abstract. End users are said to be "the weakest link" in information systems (IS) security management in the workplace. They often knowingly engage in certain insecure uses of IS and violate security policies without malicious intentions. Few studies, however, have

examined end user motivation to engage in such behavior. To fill this research gap, in the present study we propose and test empirically a non-malicious security violation (NMSV) model with data from a survey of end users at work. The results suggest that utilitarian outcomes (relative advantage for job performance, perceived security risk), normative outcomes (workgroup norms), and self-identity outcomes (perceived identity match) are key determinants of end user intentions to engage in NMSVs. In contrast, the influences of attitudes toward security policy and perceived sanctions are not significant. This study makes several significant contributions to research on security-related behavior by (1) highlighting the importance of job performance goals and security risk perceptions on shaping user attitudes, (2) demonstrating the effect of workgroup norms on both user attitudes and behavioral intentions, (3) introducing and testing the effect of perceived identity match on user attitudes and behavioral intentions, and (4) identifying nonlinear relationships between constructs. This study also informs security management practices on the importance of linking security and business objectives, obtaining user buy-in of security measures, and cultivating a culture of secure behavior at local workgroup levels in organizations.

Summary. The article focuses on addressing and correcting the actions for non-malicious security violations, which is an unconscious behavior that generates a security incident, and omissive behavior in which end users fail to adopt security behaviors that prevent security incidents. Ken, Yuan, Archer and Connelly's research shows that trying to utilize a deterrent theory to prevent non-malicious security violations or omissive behavior does not work since the individual's or group's actions are not intentional. The authors' research provides a framework for how to resolve non-malicious security violations and omissive behavior: (a) use repetition to encourage adoption of information security behaviors; (b) change the individual's or group's attitude toward information security; (c) use socialization, where individuals learn information from peers to promote the adoption of information security behavior; and (d) increase perception of risk, as individuals attempt to avoid possible information security risks (e.g., opening unsafe file attachments within email, or browsing through web sites not related to the organization). Through the authors' research of the four possible solutions to deter non-malicious security violations and/or omissive behavior, the most promising is information security behavior through socialization, as socialization has the strongest influence on individuals or groups.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C., (2014). Determining employee awareness using the human aspects of information security questionnaire (hais-q). *Computers & Security*, *42*, 165-176.

Abstract. It is increasingly acknowledged that many threats to an organisation's computer systems can be attributed to the behaviour of computer users. To quantify these human-based information security vulnerabilities, we are developing the Human Aspects of Information Security Questionnaire (HAIS-Q). The aim of this paper was twofold. The first aim was to outline the conceptual development of the HAIS-Q, including validity and reliability testing. The second aim was to examine the relationship between knowledge of policy and procedures, attitude towards policy and procedures and behaviour when using a work computer. Results from 500 Australian employees indicate that knowledge of policy and procedures had a stronger influence on attitude towards policy and procedure than self reported behaviour. This finding suggests that training and education will be more effective if it outlines not only what is expected (knowledge) but also provides an understanding of why this is important (attitude). Plans for future research to further develop and test the HAIS-Q are outlined.

Summary. This article has two areas of focus. The first focus is to create a Human Aspect of Information Security Questionnaire (HAIS-Q), and the second focus is to determine an employee’s attitude towards policies and procedures involving information security. Authors Parsons, McCormac, Butavicius, Pattinson, and Jerram were successful in creating a questionnaire to survey end users’ attitudes towards policies and procedures involving information security. One issue with the authors’ questionnaire is the fact that the questionnaire is internal to the organization, which means it carries less weight with employees and has the possibility of having some bias built into the questionnaire. The second focus of the article was to distribute the questionnaire to employees and gather data from the results in an effort to better understand the attitudes of employees towards information security policies and procedures. The authors’ data shows that 66% of those surveyed had a favorable attitude towards the information security policies, with about 78% of employees operating within the guidelines provided. A correlation was identified between attitude and behavior towards policies and procedures when this information has been shared with the employees. When the policies and procedures were shared with employees the favorable attitude and behavior of the employees towards the policies and procedures would increase by 18%. This compares to the weaker relationship between the end user and the organization’s security policies when the policies and procedures were not provided to the end users.

Training Methods

Albrechtsen, E. , & Hoyden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. *Computers & Security*, *29*(4), 432-445. doi:10.1016/j.cose.2009.12.005

Abstract. The paper discusses and evaluates the effects of an information security awareness programme. The programme emphasised employee participation, dialogue and collective reflection in groups. The intervention consisted of small-sized workshops aimed at improving information security awareness and behaviour. An experimental research design consisting of one survey before and two after the intervention was used to evaluate whether the intended changes occurred. Statistical analyses revealed that the intervention was powerful enough to significantly change a broad range of awareness and behavior indicators among the intervention participants. In the control group, awareness and behaviour remained by and large unchanged during the period of the study. Unlike the approach taken by the intervention studied in this paper, mainstream information security awareness measures are typically top-down, and seek to bring about changes at the individual level by means of an expert-based approach directed at a large population, e.g. through formal presentations, e-mail messages, leaflets and posters. This study demonstrates that local employee participation, collective reflection and group processes produce changes in short-term information security awareness and behaviour.

Summary. The article focuses on creating an information security awareness program. The authors, Albrechsten and Hoyden, advocate creating small workshops to share knowledge about information security and raise awareness through employee participation, dialogue and reflection. A survey was provided to the 100 employees who attended the workshops in advance in an effort to get a baseline on information security awareness. The 100 employees then had the opportunity to attend one of six workshops. During the workshops information was provided to the employees about information security. Then, the groups at the workshops were divided into two or three person teams to discuss and reflect on information security. After the workshop another test was provided to the 100 employees to monitor if the employees retained the information and behaviors for information security awareness. The results were clear, showing that the small workshops prove to be more valuable then large meetings or presentations with one speaker and no opportunities for interaction. The principle of workshops, like small groups, is that employee participation and the inclusion of time to reflect create a more effective learning environment.

Jenkins, J., Durcikova, A., & Burns, M. (2013). Simplicity is bliss: Controlling extraneous cognitive load in online security training to promote secure behavior. *Journal of Organizational and End User Computing*, *25*(3), 52-66.

Abstract. User-initiated security breaches are common and can be very costly to organizations. Information security training can be used as an effective tool to improve users' secure behavior and thus alleviate security breaches. Via the lens of learning, working memory, and cognitive load theories, this research examines how to improve the effectiveness of security training through decreasing extraneous stimuli in the presentation of online security training. The authors conducted a realistic laboratory experiment to examine the influence of training with different levels of extraneous stimuli on secure behavior. They found that training presented with low levels of extraneous stimuli improved secure behavior more than training presented with high levels. The results question the effectiveness of elaborate training programs, and rather suggest that simple, direct training modules are most effective.

Summary. This article describes how low levels of extraneous stimuli, such as low levels of visual information, are more effective than high levels of extraneous stimuli with regard to information security training. Jennkins, Durcikova, and Burns describe the cognitive load, which occurs when information is presented, taught and processed through the body senses and then organized by the brain and stored in short or long-term memory. Cognitive load was divided into three categories: (a) intrinsic cognitive load refers to the amount of memory required to learn; (b) germane cognitive load is working memory and how information is processed; and (c) extraneous cognitive load is information that is being presented, not information that is communicated.

The authors had participation from 238 students. These students were divided into three groups: (a) no training; (b) Low Level Extraneous Stimuli, who received a four minute presentation with only text; and (c) High Levels Extraneous Stimuli, who received a five minute presentation with audio and video. The results of the authors' research indicated that while the cognitive approach for low levels of extraneous stimuli was the most beneficial for learning new information relating to security because the information requires minimal cognitive load to be processed and stored, the results did not show a significant difference between the two approaches. The results only applied when comparing results to individuals with no training.

Karjalainen, M., & Siponen, M. (2011). Toward a new meta-theory for designing information systems (is) security training approaches. *Journal of the Association for Information Systems*, *12*(8), 518-555.

Abstract. Employees' non-compliance with IS security procedures is a key concern for organizations. To tackle this problem, there exist several training approaches aimed at changing employees' behavior. However, the extant literature does not examine the elementary characteristics of IS security training, such as the ways in which IS security training differs from other forms of training. We argue that IS security training needs a theory that both lays down these elementary characteristics and explains how these characteristics shape IS security training principles in practice. We advance a theory that suggests that IS security training has certain elementary characteristics that separate it from other forms of training, and we set a fundamental direction for IS security training practices. Second, the theory defines four pedagogical requirements for designing and evaluating IS security training approaches. We point out that no existing IS security training approach meets all of these requirements and demonstrate how to design an IS security training approach that does meet these requirements. Implications for research and practice are discussed.

Summary. This article focuses on new methods to deliver information security (IS) training. Previously there were more than 32 different approaches to delivering IS training. These methods include theories-based training, security awareness program approaches, and computer-based training. The authors state that these 32 training approaches are effective when training for specific items. For example, computer-based training is good for problem solving in response to IS incidents or as part of security awareness programs. The authors believe a new meta-theory needs to be created to train individuals about information security. The new method is made up of three components: (a) provides elementary characteristics of information security; (b) explain how these

characteristics support the IS training; and (c) create models on how to evaluate training. Meta-theory is a goal-oriented model whose purpose is to change an organization's end users' information security behaviors.

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *Mis Quarterly, 34*(4), 757-778. **Abstract.** Employee noncompliance with information systems security policies is a key concern for organizations. If users do not comply with IS security policies, security solutions lose their efficacy. Of the different IS security policy compliance approaches, training is the most commonly suggested in the literature. Yet, few of the existing studies about training to promote IS policy compliance utilize theory to explain what learning principles affect user compliance with IS security policies, or offer empirical evidence of their practical effectiveness. Consequently, there is a need for IS security training approaches that are theory-based and empirically evaluated. Accordingly, we propose a training program based on two theories: the universal constructive instructional theory and the elaboration likelihood model. We then validate the training program for IS security policy compliance training through an action research project. The action research intervention suggests that the theory-based training achieved positive results and was practical to deploy. Moreover, the intervention suggests that information security training should utilize contents and methods that activate and motivate the learners to systematic cognitive processing of information they receive during the training. In addition, the action research study made clear that a continuous communication process was also required to improve user IS security policy compliance. The findings of this study offer new insights for scholars and practitioners involved in IS security policy

compliance.

Summary. The article focuses on how to develop a strategy for an information security-training program. The authors provide two different strategies. The Elaboration Likelihood Model (ELM) focuses on behavioral and attitude changes to help process the information security content learned through different security tasks, such as changing passwords often, logging off when done with their computer session. The second training strategy offered by the authors is the Universal Constructive Institutional Theory (UCIT) model, which focuses on training relating to specific groups. An example would be customer service focused to online banking. This group has to understand web browsers' security, anti-virus software and possible firewall configuration. Both models compliment each other in training. ELM with a highly motivated student is more likely to benefit from cognitive processes, allowing users to organize and process information quickly, while a less motivated end user will benefit more from cues like reactions to the speaker, the speaker's attractiveness, or the speaker's credibility.

UCIT offers more traditional training led by an instructor, providing learning tasks and objectives. The purpose for these two training models is to maximize information security training retention and compliance, which was achieved by Puhakainen and Siponen. However, the authors state that training was not enough, and communication from senior management is still required to instill an information security culture.

Shaw, R. , Chen, C. , Harris, A. , & Huang, H. (2009). The impact of information richness on information security awareness training effectiveness. *Computers & Education*, *52*(1), 92-100. doi:10.1016/j.compedu.200806.011

Abstract. In recent years, rapid progress in the use of the Internet has resulted in huge losses in many organizations due to lax security. As a result, information security awareness is becoming an important issue to anyone using the Internet. To reduce losses, organizations have made information security awareness a top priority. The three main barriers to information security awareness are: (1) general security awareness, (2) employees' computer skills, and (3) organizational budgets. Online learning appears a feasible alternative to providing information security awareness and countering these three barriers. Research has identified three levels of security awareness: perception, comprehension and projection. This paper reports on a laboratory experiment that investigates the impacts of hypermedia, multimedia and hypertext to increase information security awareness among the three awareness levels in an online training environment. The results indicate that: (1) learners who have the better understanding at the perception and comprehension levels can improve understanding at the projection level; (2) learners with text material perform better at the perception level; and (3) learners with multimedia material perform better at the comprehension level and projection level. The results could be used by educators and training designers to create meaningful information security awareness materials.

Summary. The article focuses on how to develop an organization's information security awareness through online training. Shaw, Chen, Harris, and Huang proposed eight different hypotheses in an effort to define which training would be most beneficial using different amounts of media rich content. To identify which training method is the most beneficial, a survey was provided to 240 people; of the 240 surveys only 154 surveys were identified as valid surveys. These surveys were gathered and the data was compiled. Media was separated into three categories: (a) hypermedia, which is the richest medium that contains audio, video, graphics, plain text and links, allowing the trainee to move through the learning in a non-linear format; (b) multimedia, which also consists of graphics, audio, video, plain text and links, but the trainee is only allowed to move through the training in a linear format; and (c) hypertext, which consists of plain text and links lacking in media rich content. The authors focused on four different learning attributes: (a) feedback compatibility; (b) multiple cues; (c) language variety; and (d) personal focus in regard to the influence the training format had on learning. Shaw et al. gathered the information and grouped the data into three groups: (a) perception, (b) comprehension, and (c) projection. The surveys showed that hyper media had the most influence on an end user's ability to perceive, comprehend and project possible threats, such as spear phishing emails or malicious links that redirect end users to malicious sites. The authors believe that hyper media is a more influential platform in which to build information security awareness materials.

Conclusion

The purpose of this annotated bibliography is to identify research sources that describe how to incorporate an information security culture into an organization. Key findings are targeted towards Information Security professionals, Information Technology managers, Training and Development managers, and executives in medium to large organizations, all of whom have a vested interest in ensuring that information security cultures are successfully introduced and maintained in their organizations.

Conclusions drawn from the research are presented in three categories: (a) corporate culture, (b) end-user information security behavior, and (c) training methods.

Information Security Culture

Information security culture is simply defined as a social culture that incorporates technical information security measures (Ruighaver, Maynard, Chang, & Maynard, 2007). The successful introduction and ongoing maintenance of an information security culture is the responsibility of the organization's senior leadership, who must ensure they establish the culture throughout the organization (Da Veiga & Martins, 2015). This type of culture change cannot trickle down from the top of the organization, but rather must be actively promoted for all individuals to understand and adopt the culture (Albrechtsen & Hoyden, 2010).

Rastogi and von Selms (2012) also provide research that indicates that the introduction of an information security culture supports the development of security policies and procedures, which ultimately drives the implementation of an information security awareness program (Rastogi & von Solms, 2012). Shaw, Chen, Harris, and Huang (2009) note that an excellent channel to distribute information for a new information security culture to end-users is through the information security awareness program.

For end users to comply with information security policies and procedures, individuals must be included in the implementation, or at least notified of the upcoming change (Puhakainen, & Siponen, 2010). Parsons, McCormac, Butavicius, Pattinson and Jerram (2013) provide data that show that positive attitudes and behaviors of end users have a positive influence on adoption rates when security policies are implemented.

End-user Information Security Behavior

End users are a critical element to any organization, but end users can also be a liability when considering information security. Computer users who are not operating within the bounds set by policies and procedures create security gaps (Ken, Yuan, Archer, & Connelly, 2011).

Many information security incidents that take place are non-malicious in nature, since many end users lack the knowledge to understand what type of behavior is or is not authorized while on a network (Ken, Yuan, Archer, & Connelly, 2011). Addressing this issue requires that an organization perform two tasks (Puhakainen, & Siponen, 2010). The first task is to provide training. Information security training should provide the end users of an organization with an understanding of why information security behavior is important. Training provides the opportunity to link the business strategies with the need for information security, and training also achieves user buy-in by sharing information about policies and procedures and why they are important (Parsons, McCormac, Butavicius, Pattinson, & Jerram, 2014). Information security awareness training also provides individuals with the knowledge to understand and adopt information security behaviors into their personal lives (Albrechtsen & Hoyden, 2010). These new security behaviors will become natural and carry over into their professional lives, assisting in the security and protection of the organization's data and networks (Ken, Yuan, Archer, & Connelly, 2011).

The second task for a business is to share knowledge about information security (Albrechtsen & Hoyden, 2010). Sharing information about polices and procedures allow individuals to feel like they are part of the organization. When individuals feel like they belong to an organization they are18% more likely to accept the policies and procedures implemented by an organization (Parsons, McCormac, Butavicius, Pattinson, & Jerram, 2014). End users have a better attitude and acceptance rate when information is shared within the organization, thus assisting with the adoption of information security through socialization (Ken, Yuan, Archer, & Connelly, 2011). Peers have a stronger influence on each other, and as a result the information security culture is embedded deeper into the organization (Ken, Yuan, Archer, &

Connelly, 2011).

Training Methods

Implementation of an information security awareness program enables the provision of information security training to end users to provide the skill sets needed to reduce security incidents and transform users into security assets (Da Veiga, & Martins, 2015). There are multiple training methods, and the literature shows that there is not a consensus on the most effective approach to providing training on information security. According to Puhakainen, and Siponen, (2010), the two most effective models are Elaboration Likelihood Model (ELM), which focuses on behavior and attitudes, and the Universal Constructive Institutional Theory (UCIT) model, which is training for specific skill sets or groups. However, Albrechtsen and Hoyden (2010) state that the most beneficial type of training for individuals in developing an information security awareness program is small workshops. The authors note that workshops provide a small, intimate environment for complete participant involvement, along with positive peer influence.

As suggested by Shaw, Chen, Harris, and Huang (2009), the most consumed type of educational materials is hyper media. Hyper media uses videos, graphics, audio and links that allow end users to focus on what is important to them. This approach allows end users to move through training in a non-linear pattern, which is effective because non-linear learning allows the user to control the pace, content and sequence in which they learn about information security (Martin, 2008). In the end though, Puhakainen and Siponen (2010) note that providing training is not enough to ensure that employees embrace best practices for information security. Communication from senior management is still required to effectively instill an information security culture (Puhakainen, & Siponen, 2010).

An information security culture can assist in combatting a technological world filled with fear, unknown and doubt by establishing security policies, implementing different layers of security and providing end users with the knowledge to adopt better information security behaviors (Thomson, & von Solms, 2005). These goals are achieved by making information security a key component of an organizational culture, along with managing end user behaviors through the provision of effective training. Training is a catalyst to cultivate an information security culture (Karjalainen, & Siponen, 2011). Analytics should be utilized to monitor behavior and adoption rate to identify if the correct information is being provided, or whether changes are needed to the curriculum (Johnson & Goetz, 2007). Implementing an information security culture will increase end user security awareness and improve security behavior maximizing user productivity by reducing security incidents.

References

Albrechtsen, E. , & Hoyden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. *Computers & Security, 29*(4), 432-445. doi:10.1016/j.cose.2009.12.005

Ashenden, D. & Sasse A. (2013, November). CISOs and organizational culture: Their own worst enemy?. *Computers and Security*, *39*(B), 396-405. doi: 10.1016/j.cose.2013.09.004

Bell, C., & Frantz, P. (2014). *Critical evaluation of information sources*. Retrieved from http://library.uoregon.edu/guides/findarticles/credibility.html

Caldwell, T. (2014, June). The true cost of being hacked. *Computer Fraud & Security, 2014*(6), 8-13. doi:doi:10.1016/S1361-3723(14)70500-7

Corporate Culture. (2015). In *Dictionanary.com*. Retrieved from http://dictionary.reference.com/browse/Corporate%20Culture?s=t

Da Veiga, A., & Martins, N. (2015, March). Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers and Security*, *March (4*9), 162-176 doi: 10.1016/j.cose.2014.12.006

Fischer, E. A. (2014). *Cybersecurity Issues and Challenges: In Brief*. Retrieved from http://www.fas.org/sgp/crs/misc/R43831.pdf

Grobauer, B., Walloschek, T., & Stocker, E. (2011, March). Understanding cloud computing vulnerabilities. *Security & Privacy, IEEE , 9*(2), 50-57. doi:10.1109/MSP.2010.115

Hardikar, A. (2008). *Malware 101 - Viruses*. SANS. Retrieved from http://www.sans.org/reading-room/whitepapers/incident/malware-101-viruses-32848

Hasib, M. (2013). *Impact of Security Culture on Security Compliance in Healthcare in the USA*. Charleston, SC: CreateSpace LLC.

Huigang, L. & Yajiong, X. (2010). Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective. *Journal Of The Association For Information Systems*, *11*(7), 394-413.

IBM. (2014). *2014 Cost of Data Breach Study: Global Analysis*. Retrieved from http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&appname=GTSE_SE_SE_USEN&htmlfid=SEL03027USEN&attachment=SEL03027USEN.PDF#loaded

Jenkins, J., Durcikova, A., & Burns, M. (2013). Simplicity is bliss: Controlling extraneous cognitive load in online security training to promote secure behavior. *Journal of Organizational and End User Computing*, *25*(3), 52-66.

Johnson, M.E., & Goetz, E. (2007, June). Embedding information security into the organization. *Security & Privacy, IEEE , 5*(3), 16-24. doi:10.1109/MSP.2007.59

Karjalainen, M., & Siponen, M. (2011). Toward a new meta-theory for designing information systems (is) security training approaches. *Journal of the Association for Information Systems, 12*(8), 518-555.

Ken H, G. , Yuan, Y. , Archer, N. , & Connelly, C. (2011). Understanding non-malicious security violations in the workplace: A composite behavior model. *Journal of Management Information Systems*, *28*(2), 203-236.

Koch, H., Leidner, D. E., & Gonzalez, E. S. (2013). Digitally enabling social networks: resolving IT-culture conflict. *Information Systems Journal*, *23*(6), 501-523. doi:10.1111/isj.12020

Krausz, M., & Walker, J. (2013). *The True Cost of Information Security Breaches and Cyber Crime*. n.p.: IT Governance Ltd.

Lennon, M. (2015). *Hackers Hit 100 Banks in 'Unprecedented' $1 Billion Cyber Heist: Kaspersky Lab*. Retrieved from http://www.securityweek.com/hackers-hit-100-banks-unprecedented-1-billion-cyber-attack-kaspersky-lab

Martin, F. (2008). Effects of practice in a linear and non-linear web-based learning environment. *Journal of Educational Technology & Society*, *11*(4), 81-93.

Mitra, S., & Ransbotham, S., (2009). Choice and chance: A conceptual model of paths to information security compromise. *Information Systems Research, 20*(1), 121+. Retrieved from http://go.galegroup.com/ps/i.do?id=Gale%7CA197186605&v=2.1&u=s8492775&it=r&p=AONE&sw=w&asid=7c5793a220f2c60310fcb17048a2fe80

National Security Telecommunications and Information Systems Security Committee. (2000). *National Information Systems Security Glossary*. Retrieved from http://handle.dtic.mil/100.2/ADA433929

National Institute of Standards and Technology. (2010). *Guide for Assessing the Security Controls in Federal Information Systems and Organizations*. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf

Online Trust Alliance. (2015). *Security and Privacy Enhancing Best Practices*. Retrieved from https://www.otalliance.org/system/files/files/resource/documents/ota2015-bestpractices.pdf

Organization Economic Cooperation and Developlment. (2004). *OECD Principles of Corporate Governance*. Retrieved from http://www.oecd.org/daf/ca/corporategovernanceprinciples/31557724.pdf

Parsons, K. , McCormac, A. , Butavicius, M. , Pattinson, M. , Jerram, C. , et al. (2014). Determining employee awareness using the human aspects of information security questionnaire (hais-q). *Computers & Security*, *42*, 165-176.

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *Mis Quarterly*, *34*(4), 757-778.

Rastogi, R. , & von Solms, R. (2012). Information security service culture - information security for end-users. *Journal of Universal Computer Science*, *18*(12), 1628-1642.

Ruighaver, A. , Maynard, S. , Chang, S. , & Maynard, S. (2007). Organisational security culture: Extending the end-user perspective. *Computers & Security*, *26*(1), 56-62.

SANS. (2014). *Ouch! What is Malware*. Retrieved from http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201402_en.pdf#__utma=216335632.105590904.1429762800.1429762800.1429762800.1&__utmb=216335632.5.8.1429762814185&__utmc=216335632&__utmx=-&__utmz=216335632.1429762800.1.1.utmcsr=google|utmccn=(organic)|utmcmd=organic|utmctr=(not%20provided)&__utmv=-&__utmk=213510743

Schiff, J. L. (2015). *6 Biggest Business Security Risks and How You Can Fight Back*. Retrieved from http://www.cio.com/article/2872517/data-breach/6-biggest-business-security-risks-and-how-you-can-fight-back.html

Shaw, R. , Chen, C. , Harris, A. , & Huang, H. (2009). The impact of information richness on information security awareness training effectiveness. *Computers & Education*, *52*(1), 92-100. doi:10.1016/j.compedu.200806.011

Thomson, K. , & von Solms, R. ,(2005). Information security obedience: A definition. *Computers & Security*, *24*(1), 69-75. doi:10.1016/j.cose.2004.10.005

Van Niekerk, J. F. & Von Solms, R. (2009, June). Information security culture: A management perspective. *Computers and Security*, *29*(4), 476-486 doi: 10.1016/j.cose.2009.10.00