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

Training Programs to Increase Cybersecurity Awareness and Compliance in Non-profits

CAPSTONE REPORT

John Randy Ray
Business Applications Specialist
YMCA of San Diego County

University of Oregon
Applied Information
Management
Program

December 2014

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

Approved by

_____

Dr. Kara McFall
Lecturer, AIM Program

Training Programs to Increase Cybersecurity Awareness and Compliance in Non-profits

John Randy Ray

YMCA of San Diego County

Abstract

Most non-profits accumulate and store sensitive and vital business information digitally and are becoming increasingly reliant on technology; they are therefore more at risk for cyber-attacks (Goldernberg, 2013). Despite technical cybersecurity efforts, the employee remains the most vulnerable target for cyber-criminals (Hu, Dinev, Hart, & Cooke, 2012). Educating employees through cybersecurity awareness programs ultimately contributes to an organization's cybersecurity efforts (Kolb & Abdullah, 2009). This annotated bibliography presents literature about common cybersecurity vulnerabilities, stakeholders, and training.

Keywords: nonprofit, NGO, 501c 3, 501 (c)(3), cybersecurity, cybersecurity awareness programs, data breach, cybercrime, training programs, employee behavior, information management, and risk management

Table of Contents

Introduction to the Annotated Bibliography

Problem

In the realm of cybersecurity, computer users are often referred to as "the weakest link" (Renaud & Goucher, 2014, p. 361). A report by the Ponemon Institute (2014) estimates the cost of data breaches for organizations within the U.S. increased from $5.4 million in 2013 to $5.9 million in 2014, with a 15 percent increase in customers who terminated their relationships with breached organizations. Of these breaches, 31 percent were caused by employee negligence.

Employees' risky online behaviors are responsible for many cyber-attacks and represent a considerable cause of the increase of successful cyber-attacks (Paganini, 2013). For example, "new [online] business opportunities, mobile platforms, clouds and social media are considered privileged vectors to reach a wide audience unaware of cyber threats" (Paganini, 2013, para. 38). The types of risky behavior that result in security breaches include:

- Not logging out of application accounts
- Sharing login credentials
- Accepting request forms from unknown parties (Paganini, 2013)
- Phishing emails
- Stolen devices (Ranger, 2014)
- Falling victim to social engineering, defined as "the art of gaining trust or acceptance in order to persuade someone to provide information or perform an action to benefit the attacker" (Thomas, 2014, para. 2)
- Bad password practices (Athitakis, 2014)

- Poor web surfing decisions such as clicking on malvertisements (Blue, 2014), which are defined as "a malicious variety of online advertisements generally used to spread malware" (Donohue, 2014, para. 1).

Employees are an organization's first line of defense against cybercrime, but they are also the greatest security risk and the most common cause of data breaches (Devaney & Stein, 2012). In discussing information security within an organization, Caldwell (2013) notes:

> "The most at-risk personnel are uninformed, innocent and unaware employees," says Kevin Bailey, Research Director, European Security Software, at research company IDC.
>
> "Many external attacks – more than 60% - target employees via social engineering" he says. "They were opportunistic, exploiting activities such as unexpected communication through email and social media" (para. 3).

The laissez-faire attitude towards cybersecurity is seen not only with low to mid-level employees, but also with upper level management and board members. According to The Honorable Tom Ridge, CEO of the security firm Ridge Global and the first Secretary of the U.S. Department of Homeland Security, too many leaders view cybersecurity as just an information technology [IT] problem, a dangerous and widely held misconception (Epstein, 2014, p. 32). Ridge further explains, "cybersecurity is the responsibility of senior leaders who are responsible for creating an enterprise-wide culture of security" (Epstein, 2014, p. 33). This idea is expanded upon by Posthumus and von Solms (2004), who state "information security governance is a complex issue requiring the commitment of everyone in an organization to do their bit in order to protect their company's valuable business information assets" (p.646).

Organizations may not fully eliminate cyber risk, but they can manage it and make more effective cybersecurity investment decisions by being educated about cyber issues and clearly

understanding what their adversaries seek and what their motivations are (Epstein, 2014, p. 33). Employees are a crucial factor in ensuring the security of computer systems and valuable information resources. Human actions account for a far greater degree of computer-related loss than all other sources combined (Guttman & Roback, 1995). Brodie (2009) suggests that many potential cyber-breach problems that could affect an organization's infrastructure can be prevented if employees are informed about the issues of risks (p. 19).

Large for-profit businesses and government agencies are not the only entities susceptible to lax cybersecurity practices by their employees; non-profits are also prone to cyber-attacks due to employee error (Parker, 2014). For example, in 2013 an employee at the non-profit organization People Plus, a health and wellness organization for older adults, posted the organization's donor database to their website, which showed the addresses, phone numbers, birthdates and other personally identifiable information of their donors (Cohen, 2013). In addition to engaging in risky online behavior and being digitally unaware, non-profit employees also downplay the possibility that their organizations could be targets for cyber-attacks. Zackal (2014), a cybersecurity expert, explains that non-profit employees think cybersecurity is not overly important, as the employees do not view their organizations as valuable targets for cyber-crime. In general, "[all] organizations are misjudging the severity of risks they face from cyber attacks from a financial, reputational, and regulatory perspective" (Armerding, 2013, para. 6).

The cost of cybersecurity breaches can be high for non-profits. As Goldernberg (2013) states, an organization's operations can be severely impacted by a cybersecurity breach, and such occurrences will inhibit expanding mission efforts for most non-profits. Most non-profits, churches and NGO organizations maintain and accumulate sensitive and personal information about their members, store vital business information in digital format and are

becoming increasingly more reliant on technology, all of which puts these organizations more at risk for cyber-attacks by individuals who may wish to damage the reputations and operations of these organizations (Goldenberg, 2013).

Purpose

One intent of this study is to identify sources that build the case for the implementation of a cybersecurity awareness program within a non-profit organization. This literature review highlights various cyber-attacks and weaknesses faced and caused by employees, and includes sources that explain the current cyber-threat environment most industries face. Literature is presented that details specific cybersecurity risks faced by non-profits; specifically threats that target the employee, illustrating the need for all employees to adhere to good cybersecurity practices.

Another key goal of this study is to identify sources that stress the need for executive and board leadership in the governance of cybersecurity. Research is presented that shows the key roles executive leaders play in securing resources and support for cybersecurity programs in order to effectively mitigate threats (Epstein, 2014).

Finally, reference sources are provided that present training models, that lay the groundwork for developing and implementing effective cybersecurity awareness programs and encourage the intended employee behavior in regard to an organization's cybersecurity efforts. Emphasis is placed on sources that suggest specific training tools, processes and theories for implementing cybersecurity awareness programs.

Research Question

Main question. What training model(s) are shown to be effective for non-profit organizations to encourage increased cyber-awareness levels for employees and guide preferred employee behavior in regard to cybersecurity efforts?

Sub-questions. What constitutes a data breach and what cyber-risks do employees commonly face? Who should be involved in forming cyber-awareness programs? What training frameworks and tools effectively target employee behavior to increase cyber-awareness?

Audience

The audience members for this study are primarily individuals who work for non-profits. As Basu (2014) states, "each person on a company's management team must be armed with the requisite knowledge to make informed decisions about cybersecurity – not just an understanding of the basic concepts" (para. 5). These individuals include the Chief Information Officers (CIOs), technology managers, Legal Counsels, Chief Human Resource Officers, Training Officers, key executive directors and non-profit board members. Those who serve in these or similar roles are instrumental in the development and implementation of cyber-awareness programs.

In most organizations, it is the CIO's responsibility to develop and implement information technology initiatives, as well as manage technical staff. The CIO may be viewed as the point person to provide information regarding the current state of an organization's information security efforts and to develop the visions and tactical initiatives for the implementation of cybersecurity programs.

This annotated bibliography is also for persons who serve in Legal Counsel positions as it provides information regarding the legal landscape of cybersecurity, data breaches and data

privacy regulations. For example, California was the first state to mandate data breach notifications and currently businesses are required to report any breach involving more than 500 California residents (Harris, 2014). Legal Counsel will glean insights into how organizations can prepare themselves from a legal standpoint for potential security breaches, as well as identify any probable legal risks their organizations might face.

Human Resources and Training Officers will need to understand how to incorporate any cybersecurity initiatives within their organizations' current training and onboarding structures. They also need to provide input into HR policy changes which incorporate cybersecurity practices and requirements.

Finally, this annotated bibliography is for persons who serve as a member of a board of management as it highlights how boards may spur a culture of cybersecurity awareness. Board members have a responsibility to guide their organizations towards developing appropriate cybersecurity frameworks.

Search Strategy

Information regarding the problem and audience is collected through various search sources and methods, which include:

A) **University of Oregon Libraries website.** Searches within this site are focused on discovering peer-reviewed journals, articles and case studies that provide information which describes or relates to the problem. Searches specifically target literature on non-profits; however, other industries are considered if the information presented defines or explains common cybersecurity issues faced by most industries.

B) **Databases.** By utilizing the *quick search* function in the "articles, databases, indexes" section of the University of Oregon Libraries website, the following databases provide results:

- Academic Search Premier
- Project Muse
- Web of Science

However, queries, which provide the most relevant resources, are subject specific database searches. For example, searching the subject "Business" provides results from:

- Business Source Complete
- EconLit
- Factiva
- Regional Business News

C) **Google Scholar & Google.** Searches using Google and Google Scholar are used to find information regarding the current state of cybersecurity within the U.S., individuals responsible for cybersecurity within these organizations and relevant training programs that focus on employee behavior, which helps to describe the problem and identify the audience. Selected information is limited to professional IT and Information Security websites that provide research statistics on cybercrime and the current state of cybersecurity, as well as government and industry specific websites whose focus is on IT and business management, cybersecurity, information security, cybersecurity awareness and non-profits.

D) **Amazon.com.** Searches through Amazon.com provide access to preview books and publications which are not electronically available through the University of Oregon Libraries databases.

E) **Twitter.** Twitter is used to find recent news sources and identify professional industries that report on issues and trends within cybersecurity.

Keywords. The above searches utilized combinations of the following keywords and their derivatives: *nonprofit, NGO, 501c 3, 501 (c)(3), cybersecurity, cybersecurity awareness programs, data breach, cybercrime, training programs, employee behavior, information management,* and *risk management*

Reference evaluation criteria. References are evaluated using the frameworks provided by Bell and Frantz (2014) to determine the credibility of an information source. The following credibility areas are considered:

(a) Authority – evaluated based on the author's experience within the field of IT, typically ten years or more with his or her chosen organization or within the IT industry; and whether the sources are published in peer-reviewed journals and books or the author contributes frequent articles to professional organizations.

(b) Objectivity – sources are evaluated on their merits to define, explain or explore a topic that is supported by current and past research or cited sources. Articles and research by corporate entities are considered after determining the authors' authority and determining if the sources are referenced by other credible sources.

(c) Quality – determined based on the author's ability to thoroughly explain and support arguments and points made within an article with supporting research and trends. Quality is also determined by evaluating an article's use of correct grammar and absence of spelling and typographical errors.

(d) Currency – Due to the nature of technology and cybercrime, articles with publication dates over five years are not considered as they reference outdated laws, statistics, threats and technology. Articles selected are published from 2010 – 2014.

(e) Relevancy – articles chosen are scholarly, peer-reviewed works, government reports and published books, which define, explain and explore recent trends and developments.

Annotated Bibliography

This annotated bibliography introduces 15 references that provide the groundwork for developing a cybersecurity awareness program for non-profits. The selected references are intended to help CIOs and technology managers understand the cyber challenges and threats facing employees and provide resources on how to develop a case for and implement a cybersecurity awareness program. References are presented in three categories: (a) presentation of common cybersecurity vulnerabilities, (b) who to involve in the development and governance of a cybersecurity awareness program, and (c) training structures considered effective in adjusting employee cybersecurity behaviors.

Annotations are supported by three criteria: (a) full bibliographic citation, (b) literature abstract or description of the literature, and (c) summary of the literature. The abstracts presented are complete as published. For literature without abstracts, a description of the work has been provided. Summaries provide a synthesized review of content with a focus on elements that

support the purpose of this research. The intended outcome of this annotated bibliography is to assist non-profit IT managers in their development of cybersecurity awareness trainings.

Common cybersecurity vulnerabilities

Abraham, S., & Chengalur-Smith, I. (2010, August). An overview of social engineering malware: Trends, tactics, and implications. *Technology in Society, 32,* 183-196. http://dx.doi.org/10.1016/j.techsoc.2010.07.001

Abstract. Social engineering continues to be an increasing attack vector for the propagation of malicious programs. For this article, we collected data on malware incidents and highlighted the prevalence and longevity of social engineering malware. We developed a framework that shows the steps social engineering malware executes to be successful. To explain its pervasiveness and persistence, we discuss some common avenues through which such attacks occur. The attack vector is a combination of psychological and technical ploys, which includes luring a computer user to execute the malware, and combating any existing technical countermeasures. We describe some of the prevalent psychological ploys and technical countermeasures used by social engineering malware. We show how the techniques used by purveyors of such malware have evolved to circumvent existing countermeasures. The implications of our analyses lead us to emphasize (1) the importance for organizations to plan a comprehensive information security program, and (2) the shared social responsibility required to combat social engineering malware.

Summary. This study describes the various channels in which malware, a growing cybersecurity vulnerability, is distributed and how malware is implemented from user

initiation to propagation. The article also describes how malware attacks are targeted towards users and discusses social engineering malware trends and tactics. The authors recommend periodic awareness education to reduce the risk of employees falling victim to socially engineered malware tactics. The research suggests employers need to develop periodic cyber-awareness trainings as the cyber-threat landscape changes frequently. The authors also recommend that employers should develop an ongoing information security program that caters to employees at all levels. The article directly ties to the focus of this research study by outlining common cybersecurity vulnerabilities and recommendations for mitigating the vulnerabilities.

Choo, K. (2011, November). The cyber threat landscape: Challenges and future research directions. *Computers & Security*, *30*, 719-731. http://dx.doi.org/10.1016/j.cose.2011.08.004

Abstract. Cyber threats are becoming more sophisticated with the blending of once distinct types of attack into more damaging forms. Increased variety and volume of attacks is inevitable given the desire of financially and criminally-motivated actors to obtain personal and confidential information, as highlighted in this paper. We describe how the Routine Activity Theory can be applied to mitigate these risks by reducing the opportunities for cyber crime to occur, making cyber crime more difficult to commit and by increasing the risks of detection and punishment associated with committing cyber crime. Potential research questions are also identified.

Summary. This article describes the cyber-threat landscape as it relates to financially-motivated cyber-criminal activities. It details how the common cybersecurity threats of

malware, malware on mobile devices (mobile malware), and phishing attacks are deployed and carried out and illustrates the negative consequences faced by organizations and their employees after successful attacks. It details that victims of cyber-crimes are often unaware they have experienced cyber-attacks and explains why most cyber-attacks go unreported. The author reports that cybersecurity is seen as a priority by countries such as Australia and the U.S., and points out the current challenges in cybersecurity such as a deficient workforce of cybersecurity professionals. The author provides insight into how government and private sectors can collaborate to foster a culture of cybersecurity and encourages joint user awareness and education initiatives dedicated to the topic of cybersecurity. This article directly ties to the topic of research because it highlights and describes prominent threats users (employees) face such as malware, malicious mobile apps, and point of sale and phishing attacks. It promotes the fostering of a culture of security and the implementation of user awareness and education initiatives to help organizations improve their cybersecurity efforts.

Grawemeyer, B., & Johnson, H. (2011). Using and managing multiple passwords: A week to a view. *Interacting with Computers*, *23*, 256-267. http://dx.doi.org/doi:10.1016/j.intcom.2011.03.007

Abstract. Security policies are required that protect information from unauthorised access, and also respect challenges users face in creating, and particularly managing, increasing numbers of passwords. This paper investigates *real* password use in the context of daily life. It presents the results of an empirical study where participants completed a password diary over 7 days, followed by debrief interviews to gain further

knowledge and understanding of user behaviour. The results reported relate to how many passwords are in use, the types of passwords participants created, the relationships between different passwords and to sensitive services, how participants retrieved their passwords and finally, the different strategies adopted by users in their management of passwords. The paper concludes by providing a high level set of password guidelines, along with suggestions for mechanisms to support creating, encoding, retrieving and executing multiple passwords.

Summary. This article describes the user behavior behind poor password management, a key cybersecurity vulnerability. The authors posit that most enterprise password policies fail because they are not created with the user in mind. The research focuses on the challenges of maintaining multiple passwords by chronicling the password use of 22 individuals ages 20-49 with various levels of IT knowledge over seven days to understand user perception and use of passwords. The study indicates user education is needed to explain, from a technical viewpoint, what strong passwords are, and to illustrate the best practices for creation and use. The research provides insight into understanding a key cybersecurity vulnerability and how to prevent the vulnerability by using categorization techniques as a strategy to help with the creation and memorization of passwords.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L., & Downs, J. (2010). *Who falls for phish?: A demographic analysis of phishing susceptibility and effectiveness of interventions*. Paper presented at the Proceedings of the SIGCHI Conference on Human

Factors in Computing Systems, New York, NY. Abstract retrieved from http://doi.acm.org/10.1145/1753326.1753383

Abstract. In this paper we present the results of a roleplay survey instrument administered to 1001 online survey respondents to study both the relationship between demographics and phishing susceptibility and the effectiveness of several anti-phishing educational materials. Our results suggest that women are more susceptible than men to phishing and participants between the ages of 18 and 25 are more susceptible to phishing than other age groups. We explain these demographic factors through a mediation analysis. Educational materials reduced users' tendency to enter information into phishing webpages by 40% percent; however, some of the educational materials we tested also slightly decreased participants' tendency to click on legitimate links.

Summary. This article examines user demographics to determine which group is more susceptible to engaging with phishing e-mails, a common source of cybersecurity vulnerability. This study also tested various anti-phishing education modules to determine their effectiveness on user behavior. Results of the study show women are more susceptible than men to phishing emails; however, age, education and risk behavior also play key roles in determining if users are more prone to falling for a phish. Results of the study show a combination of anti-phishing education material to be the most effective in reducing user’s susceptibility to engaging with a phish. The article describes a common cybersecurity vulnerability, provides insight into the response of targeted demographics of potential victims, and offers insight into preventing these types of attacks. The article directly ties to the focus of this research study by identifying a common cyber-risk faced by employees.

Cyber-awareness program stakeholders

Bissell, K. (2013, March). A strategic approach to cybersecurity. *Financial Executive*, *29*(2), 36-41. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=85919964&site=ehost-live&scope=site

Abstract. The article looks at threats to cybersecurity, or computer and Internet security, as of 2013, focusing on what business executives need to know and steps they should consider taking to protect their companies. It notes that cyber criminals have become much better able to carry out cyber attacks in recent years, and says many companies have not developed cyber protection policies to the extent they should. Topics include advanced persistent threats (APTs), or long-term cyber attacks, the assessment of cybersecurity risks, cyberinsurance, and proposed U.S. government regulations on cybersecurity.

Summary. This article explains how organizations need to react regarding cybersecurity threats as the cost to commit cybercrime continues to fall. The lower cost of cybercrime tools now allows for more malware disbursement and more cybercrime. The author details the monetary loss to companies and individuals in the U.S. through cybercrime and states that chief officers, board members and financial executives are key stakeholders who need to become more knowledgeable about cybercrime and learn how to better protect their organizations. Within this article, the author defines cybercrime, provides ten items regarding cybersecurity on which board members should focus to improve their organizations' cybersecurity efforts, and provides a framework for CEOs,

CIOs and financial officers to follow in order to assess their cyber-risks and promote the importance of cybersecurity.

Data Security and Breach Notification Act of 2014, S. 1976, 113th Cong. (2014).

Description. To protect consumers by requiring reasonable security policies and procedures to protect data containing personal information, and to provide for nationwide notice in the event of a breach of security.

Summary. The Data Security and Breach Notification Act of 2014 is a bill currently being presented to the U.S. Senate and House of Representatives that will require entities that store or operate with third parties who store consumers' personal information to follow designated policies and procedures regarding data security. Within the required policies, entities are required to identify individuals who will act as the points of contact and are responsible for the entities' information management. Entities must also have procedures which document their vulnerabilities and processes for correcting vulnerabilities. The bill defines the timelines and methods for entities to report a data breach and penalties entities will face if they fail to properly report a breach. Those who conceal a breach will be fined $1,000 or more per individual and will face up to five years of jail time. The bill defines what a breach of security is and identifies items that are classified as personal information. This source provides key information into who the government deems as key organizational stakeholders responsible for addressing cybersecurity.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012, August). Managing employee compliance with information security policies: The critical role of top management and organizational

culture. *Decision Sciences Journal*, *43*, 615-659. http://dx.doi.org/10.1111/j.1540-5915.2012.00361.x

Abstract. We develop an individual behavioral model that integrates the role of top management and organizational culture into the theory of planned behavior in an attempt to better understand how top management can influence security compliance behavior of employees. Using survey data and structural equation modeling, we test hypotheses on the relationships among top management participation, organizational culture, and key determinants of employee compliance with information security policies. We find that top management participation in information security initiatives has significant direct and indirect influences on employees' attitudes towards, subjective norm of, and perceived behavioral control over compliance with information security policies. We also find that the top management participation strongly influences organizational culture which in turn impacts employees' attitudes towards and perceived behavioral control over compliance with information security policies. Furthermore, we find that the effects of top management participation and organizational culture on employee behavioral intentions are fully mediated by employee cognitive beliefs about compliance with information security policies. Our findings extend information security research literature by showing how top management can play a proactive role in shaping employee compliance behavior in addition to the deterrence oriented remedies advocated in the extant literature. Our findings also refine the theories about the role of organizational culture in shaping employee compliance behavior. Significant theoretical and practical implications of these findings are discussed.

Summary. The authors indicate that employees account for more information security disruptions than outside attacks alone and they are potentially more dangerous to an organization because of their working knowledge of their organizations. They also state that employees' noncompliance to security policies can be disastrous for an organization and point out that employees are the weakest point in any information security model. The authors note that when developing any successful cybersecurity initiatives, the most challenging component is establishing an awareness program.

Within this study, the authors investigate how top management can influence the information security compliance behavior of its employees. The study explains that management's participation has significant direct and indirect influences on employee attitudes and heavily influences the organizational culture. The authors note that there has been significant research on what causes noncompliance behaviors in employees and how to manage this issue, but not enough research has been performed on the combined effects of organizational culture and management involvement on employee behavior. This study attempts to answer:

(a) What is the role of organizational culture in shaping employee intention to comply with information security policies?

(b) How does top management influence employee intention to comply with information security policies?

The research also points out that organizational culture can be influenced and managed by top management and that organizational culture in turn shapes and guides employee behavior via shared values and commitment to the organization. The authors also conclude from the study that employees who perceive their workplace to be dominant in

human relations values are more likely to accept change and report higher levels of satisfaction. The research also supports the fact that leaders can shape cultural norms based on what they focus their attention on, how they react to crises, the behavior they model and who they hire into their organizations.

Within this study, the main frameworks and models found to influence information security behavior are cognitive theories and criminological theories, but the authors declare that developing an information security culture involves two components: (a) The shared assumption about information security and (b) The education of these shared assumptions among the members of the organization.

The purpose of this study is to present how top management, a key stakeholder in cybersecurity, could shape employee information security compliance intentions directly and indirectly in conjunction with organizational culture values.

The research finds that the perceived passiveness of top management in promoting and following established information security policies is one reason employees ignore security policies. As top management attitudes change concerning information security and they become more actively engaged, measurable changes can be seen in employee attitudes and behaviors around information security policies.

Imboden, T. R., Phillips, J. N., Seib, J., & Fiorentino, S. R. (2013). How are nonprofit organizations influenced to create and adopt information security policies. *Issues in Information Systems, 14*, 166-173. Retrieved from http://iacis.org/iis/2013/269_iis_2013_166-173.pdf

Abstract. As news of cyber attacks and data breaches at corporate and government institutions have increased in frequency, the discussion as to whether nonprofit organizations are affected similarly has largely been omitted. While at first glance a typical nonprofit might not seem as valuable of a target to hackers and cyber criminals as business or public sector groups, this study finds that these organizations routinely collect and store data often targeted by digital thieves. But are they storing, transmitting, and processing this data in a safe and secure manner? The creation and adoption of a formal information security policy is often seen as the starting point for a strong information security program at an organization. This study explores the adoption as well as attitudes regarding information security policies at nonprofit organizations in two areas of Illinois.

Summary. The authors explain that there has been little research to determine if cyber-attacks and data breaches for non-profit organizations have increased at the same rate as corporate and government organizations. The study investigates information security policies and attitudes at selected non-profits. The author recognizes that human error is often overlooked in assessing cyber risk.

As non-profits continue to rely on technology to conduct business, it puts them more at risk for cybercrime. The study explains that non-profits and small to medium size organizations face similar challenges in regard to insufficient resources to dedicate towards information security. The author recommends non-profit management and technology leaders adopt an information security policy as a fundamental starting point in developing an information security infrastructure; however, the author notes that non-profits need to also develop security awareness programs for employees, as they are often the weakest link in any security initiative. The study posits that regardless of resources or

budget size, non-profits should focus on the development of information security policies and routine training of these policies and practices with their employees. This article defines the roles of non-profit management, technology leaders, and employees in preventing cybersecurity breaches.

Rai, S. (2014). *Cybersecurity what the board of directors need to ask*. Retrieved from https://na.theiia.org/special-promotion/PublicDocuments/GRC-Cybersecurity-Research-Report.pdf

Description. This report provides insight into board engagement in regard to cybersecurity efforts and introduces a framework for developing risk management around cybersecurity. As cyber attacks pose a risk for organizations, board members need to understand those risks in order to address current cybersecurity risks and anticipate future risks.

Summary. This report investigates board member perceptions regarding cybersecurity and shows awareness by board members of cybersecurity has increased; however, the roles played by board members and their involvement in cybersecurity issues have remained low. Over 50% of the board members surveyed indicated they should be actively involved in cybersecurity matters. The report outlines security items board members should consider in order to provide oversight of cyber risks. These principles are:

(a) Understand cybersecurity is an enterprise-wide-risk management issue, not just an IT issue.

(b) Understand the legal implications of cyber risks.

(c) Have adequate access to cybersecurity expertise and include discussions regarding cyber-risk on the agendas of board meetings.

(d) Set the expectation that management will establish an enterprise-wide-risk management framework with adequate staffing and budget.

(e) Discuss how to manage the different types of cyber risk.

The author explains how boards may act on these principles as well as provides resources regarding information security, data breach laws and descriptions of third party risks that board members may reference. The report concludes with a set of questions and action items board members should ask in order to prepare for an internal cybersecurity audit.

Training frameworks and tools that effectively target employee behavior to increase cyber-awareness

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology, 33,* 237-248. http://dx.doi.org/10.1080/0144929X.2012.708787

Abstract. Operating systems and programmes are more protected these days and attackers have shifted their attention to human elements to break into the organisation's information systems. As the number and frequency of cyber-attacks designed to take advantage of unsuspecting personnel are increasing, the significance of the human factor in information security management cannot be understated. In order to counter cyber-attacks designed to exploit human factors in information security chain, information security awareness with an objective to reduce information security risks that occur due to human related vulnerabilities is paramount. This paper discusses and evaluates the

effects of various information security awareness delivery methods used in improving end-users' information security awareness and behaviour. There are a wide range of information security awareness delivery methods such as web-based training materials, contextual training and embedded training. In spite of efforts to increase information security awareness, research is scant regarding effective information security awareness delivery methods. To this end, this study focuses on determining the security awareness delivery method that is most successful in providing information security awareness and which delivery method is preferred by users. We conducted information security awareness using text-based, game-based and video-based delivery methods with the aim of determining user preferences. Our study suggests that a combined delivery methods are better than individual security awareness delivery method.

Summary. The author explains that cyber security threats that exploit human behavior are constantly evolving and people tend to be the contributing factor to security violations. The author highlights this point by referencing a high profile attack on Google caused by an employee who mistakenly clicked on a phishing email. The author states that organizations need to develop and promote effective information security programs in response to the evolving laws and regulations focused on information security threats. The study investigates various channels in which security awareness trainings can be delivered; the author concludes that the critical success factor for a security awareness program is the method of delivery. This study focuses on which delivery method is preferred by users. The author notes that one of the biggest challenges with security awareness programs is that the delivery methods are not fully developed.

The author describes the following delivery methods:

(a) Conventional delivery –may consist of electronic and paper based resources to provide information on security related issues. This method runs the risk that people will not read or comprehend the information presented.

(b) Instructor-led delivery – this method consists of formal presentations facilitated by a security expert. This approach has the advantage of modifying content based on student need and timely response to questions. Its drawbacks are costs, challenges in ensuring employees are engaged, and the fact that the learning is based on employees using rote memory and not actively thinking about how to apply the concepts.

(c) Online delivery –includes e-mails, interactive meetings or chat sessions and various other multimedia platforms. The author suggests that this model is best for supporting multimodal teaching methods. The challenge in online methods is measuring the effectiveness, developing the delivery method and the possible costs associated with them.

(d) Game based delivery – delivers information security concepts via a gaming platform and may have mixed results as far as retention of information learned.

(e) Video-based delivery –educational videos that are a variant of instructor-led training. The employee is able to learn the information independently and the videos can be watched and re-watched. However, this method may run the risk of being expensive to develop or having a difficult time garnering engagement.

(f) Simulation-based delivery – subjects employees to simulated environments where information security threats are presented; employees must actively participate while educational material is presented during the simulation.

A research study was conducted that had participants engage in security awareness programs utilizing online video, game-based and text-based delivery methods. The results show that participants preferred video-based training followed by text–based training; game delivery ranked last. While the video delivery was preferred, the use of all of the delivery models provided users with a clearer understanding of security issues. The author concludes that providing just one delivery channel for employees may be easy for the organization but it may not be as effective as providing multiple delivery channels.

Chen, Y., Ramamurthy, K., & Wen, K. (2012, Winter). Organizations' information security policy compliance: stick or carrot approach? *Journal of Management Information Systems*, *29*(3), 157-188. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=cph&AN=85985309&login.asp&site=ehost-live&scope=site

Abstract. Companies' information security efforts are often threatened by employee negligence and insider breach. To deal with these insider issues, this study draws on the compliance theory and the general deterrence theory to propose a research model in which the relations among coercive control, which has been advocated by scholars and widely practiced by companies; remunerative control, which is generally missing in both research and practice; and certainty of control are studied. A Web-based field experiment involving real-world employees in their natural settings was used to empirically test the model. While lending further support to the general deterrence theory, our findings highlight that reward enforcement, a remunerative control mechanism in the information systems security context, could be an alternative for organizations where sanctions do not

successfully prevent violation. The significant interactions between punishment and reward found in the study further indicate a need for a more comprehensive enforcement system that should include a reward enforcement scheme through which the organizational moral standards and values are established or reemphasized. The findings of this study can potentially be used to guide the design of more effective security enforcement systems that encompass remunerative control mechanisms.

Summary. The study aims to identify how the use of punishment and reward systems helps to improve employee compliance with information security policies. Specifically, it examines the relationship between the certainty of control (how aptly will a reward or punishment be enforced), severity of punishment and significance of reward to determine how the combination of these systems will affect employees' security policy compliance. The authors recognize that employee negligence and insider breaches put an organization's security efforts at risk and that security technologies alone will not make an organization secure. They also observe that while most organizations are required to comply with regulations such as the Payment Card Industry Data Security Standard, Gramm-Leach-Bliley Act, Sarbanes-Oxley Act, and Health Insurance Portability and Accountability Act, most employees are not motivated to follow an organization's security policies and procedures and are opposed to adjusting their behaviors in order to comply with policies. Therefore, most organizations rely on a punishment model to enforce information security compliance.

The study describes the benefits and drawbacks of punishment and reward systems. For example, the authors cite that punishment serves to uphold social norms, signal appropriate and inappropriate behaviors and deter deviant acts, all of which help to

promote positive outcomes. However, they also cite the fact that punishment can have negative consequences such as heightening employee anxiety, aggressiveness and withdrawal behavior. Additionally, employees may display hostility or retaliate against the punishing agent. On the subject of rewards, the authors state that a reward system can create a more harmonious environment and may have a stronger effect on employee performance and increased job satisfaction. However, rewards may also be seen as manipulative and could generate a tense work environment if others are not also being equally rewarded, as rewards are based on a supervisor's discretion. Another negative outcome of rewards is the fact that employee behavior may focus more on obtaining the reward than focusing on the organization's overall objectives.

This study included the development of a punishment and reward experiment which examined people's likely behavior towards different combinations of high and low reward and punishment severity models. The authors set out to test their hypotheses that employees' intention to comply with security policies is based on the levels of both rewards and punishments. Their study supported their hypothesis that punishment combined with certainty and intention will affect employee behavior, but their hypothesis that reward combined with certainty and intention was not supported.

Clarke, N., & Furnell, S. (2012). Creating a security culture development plan and a case study. In O. Olivos (Ed.), *Proceedings of the sixth international symposium on human aspects of information security & assurance HAISA 2012*. *HAISA* (pp. 13-32). Retrieved from http://www.cscan.org/default.asp?page=openaccess&eid=13&id=28

Abstract. When developing training and awareness programs, information security specialists usually fail to consider the human element as an important component of the program (Kruger et al, 2006). They tend to focus on security policies and technical aspects leaving aside the human aspect of information security. We argue that it is necessary that the characteristics of the employees (roles and learning styles), the compliance with the current policies, the state of the security culture and the mission, vision and strategic planning of the organization be considered when setting up a security culture development plan. This paper describes the steps that should be followed to develop a Security Culture and reports a case study in an organisation where the development plan was applied.

Summary. This article suggests users' learning styles and attitudes be considered when developing an effective cybersecurity training program. The purpose of this paper is to describe, at a high level, recommended steps to utilize in developing a cybersecurity culture. The paper also provides a case study, which helps to illustrate how the recommended plan is developed and implemented.

The author specifically looks at the steps involved in developing an awareness program that will reduce the risk of socially engineered attacks against employees. The article is divided into sections that: (a) describe how to evaluate security policies, (b) provide an overview on how to determine employee attitudes and perceptions regarding security, (c) describe the human resources aspects of security, (d) explain how the security culture development plan is implemented, and (e) provide information on how to measure the results of the security plan. The author explains that the purpose of the plan is to set the groundwork of the organization's information security position and the plan should

identify roles and responsibilities, identify threats and issues, as well as explain possible countermeasures. The author recommends that management is responsible for supporting the information security policy, creating policies that closely match international standard security policies such as ISO/IEC 27002 and writing policies consistently so as to not frustrate employees.

When developing a security awareness plan, the author suggests the plan have its own budget set apart from IT or physical security budgets and be seen as an investment for the organization. The author also states that a senior manager should be identified to champion the program and members from IT, HR, Marketing, Legal and Security should actively participate within the program. Those who are selected to deliver security trainings should focus on employees' higher order thinking skills such as evaluating, judging, creating and formulating ideas and work to meet people's learning styles based on Kolb's Learning Style Inventory model.

Furman, S. M., Theofanos, M. F., Choong, Y., & Stanton, B. (2012, March/April). Basing cybersecurity training on user perceptions. *IEEE Security & Privacy*, *10*(2), 40-49. http://dx.doi.org/10.1109/MSP.2011.180

Abstract. The National Initiative for Cybersecurity Education (NICE) will be conducting a nationwide awareness and outreach program to effect behavioral change. To be effective, an educational campaign must first understand users' perceptions of computer and online security. The authors' research objective was to understand users' current knowledge base, awareness, and skills. They investigated users' understanding of online security by conducting in-depth interviews with the goal of identifying existing correct

perceptions, myths, and potential misperceptions. Their findings indicate that the participants were primarily aware of and concerned with online and computer security. However, they lacked a complete skill set to protect their computer systems, identities, and information online. Providing a skill set that lets them develop complete mental models will help them to correctly anticipate and adapt the appropriate behaviors when approaching online security.

Summary. In this article, the authors explain that the typical computer users are not prepared or educated in how to deploy and use cybersecurity tools and are unaware of or do not understand cybersecurity practices. The goal of the US National Initiative for Cybersecurity Education (NICE) is to raise cybersecurity awareness and foster change in user cyber behavior so that users will think and act more securely. The authors suggest that for this type of educational awareness program to be effective, educators must understand users' views of cybersecurity.

The author presents a three-step framework geared towards changing user behavior, which includes: awareness, education and training. Training is defined as delivering information that will change people's behavior.

The authors state that users tend to engage in more risky online behavior because they believe that damaging outcomes are less likely than positive outcomes and they expect a higher frequency of rewarding online engagement. The author notes that users' mental models regarding physical representations of cybersecurity (viruses, attackers) does not map well to their virtual counterparts (spyware, adware, hackers).

To understand users' perceptions about online security, the authors conducted a study, through an interview process, which asked users:

(a) To describe their online activities

(b) To detail their experiences with online fraud

(c) To list computer security training or education they have had

(d) To provide a self-assessment of cybersecurity

(c) To define security

(d) To explain security in regard to their various online accounts

(e) To explain their familiarity with security tools and terms

(f) To define the difference between privacy and security

The results of their study show that participants have some understanding and knowledge about online security; however, there is a discrepancy between what users think they know and what they actually know about the topic. The authors argue that at a minimum users should learn the three security objectives developed by the Federal Information Processing Standards Publication 199, Standards for Security Categorization of Federal Information and Information Systems which are confidentiality, integrity and availability, as these objectives help to provide a better mental model for users to understand and effectively adapt their cybersecurity behaviors.

Gardner, B., & Thomas, V. (2014). Building an information security awareness program Defending against social engineering and technical threats (1st ed.). Retrieved from http://www.amazon.com

Abstract. Many items factor into the training cycle for an organization such as budget, management support, regulatory compliance, and amount of material. If your organization must perform training activities to satisfy regulatory compliance, use this to

deliver meaningful training material, as opposed to the absolute minimum required. Determining or adjusting the training cycle for your organization depends not only on the security division but also on the support of the management. Work closely with the senior management as you plan your training; they will provide guidance in terms of budget, training frequency, and methods. Effective information security programs have the support of the senior management, and in the long term, it's better to deliver a scaled back program that has the support of the senior management and then spend all of your time struggling with the people whose support you need.

Summary. This chapter discusses various security awareness training cycles and provides options for readers to decide which cycle makes sense for their organization to implement. The author points out that the training cycle begins with new hire training. If security awareness training is not part of the onboarding process, then it can convey that security is not a priority for the organization or the employees. The author states that at a minimum, the following topics should be discussed with new hires:

(a) Purpose of the training

(b) Highlights of the key areas of security policy

(c) The largest threats to the organization

(d) How to identify and report information security related issues

Quarterly trainings are preferred as a way to provide the most up–to-date security threats and trends, as well as to provide current issues the organization has faced. The authors suggest that organizations detail any other notable attacks that have been made public as a way to link real-world examples with covered material.

Biannual training is suggested as the minimum amount of training an organization should provide; the authors suggest that training material should be focused on critical topics to the organization's security. Critical topics vary depending on the organization, but the security training should most closely follow new hire orientation training. The purpose of biannual training is to reinforce the fundamentals without detailing each security policy. Next, the authors present continual training, which is introduced as a low cost alternative that helps to reinforce concepts taught in new hire, quarterly or biannual trainings throughout the year. Examples of continual training include informational posters which highlight key security items, digital newsletters to provide safety tips and how-tos, and lunch and learn sessions.

Point-of-failure testing is recommended if an organization cannot support quarterly trainings. Point-of-failure testing is designed to educate the employees who need it most. For instance, if an employee fails a simulated phishing or malvertisement attack, the employee should be tested again within weeks of the failure. This process is used to reinforce presented security material by requiring the employee to apply learned concepts. Point-of-failure testing may provide mixed results depending on how it's implemented.

Finally, targeted training is introduced as part of the annual training cycle. Targeted training should be presented apart from the general employee training and focus on the threats that are most relevant to a department. For example, help desk employees may receive socially engineered security threats via fake phone calls or emails regarding computer accounts, while the accounting department may be more at risk for introducing

viruses into the network from opening email attachments received from outside the organization.

The author suggests if an organization does not currently have an awareness program in place that it is best to plan for a more robust training cycle, as it may be easier to garner acceptance of a new training cycle rather than to modify one. Regardless, if the organization can support a biannual or quarterly training cycle, it is recommended that each cycle include continual and targeted training, as this approach will help to yield a higher return on investment.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014, May). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Computers & Security*, *42*, 165-176. http://dx.doi.org/Retrieved from

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. The purpose of this research is to examine the relationships between employees' knowledge of policies and procedures and their attitude toward them in order to produce a validated instrument known as the Human Aspects of Information Security Questionnaire. The authors propose that this instrument be used to measure employee knowledge, attitudes and behavior, which could provide information on the effectiveness of information technology controls.

The authors identified a gap in information security surveys, as those surveys commonly collect data about security breaches and their impacts but do not report what users think, know, or do about information security issues. They further explain that employee behavior is influenced by many factors, which include personality, the organization, and its culture.

Within the conceptual development of the HAIS-Q, the authors found that management is most concerned about employee errors in regard to information security due to ignorance and naivety rather than maliciousness. They hypothesize the following:

(a) Better knowledge of policies and procedures is associated with a better attitude towards the policies and procedures.

(b) Better attitude towards policies and procedures is associated with self-reported behavior that is more risk averse.

(c) Better knowledge of policies and procedures is associated with self-reported behavior that is more risk averse.

This study helps to increase the confidence of employers in the notion that improving employees' knowledge of policies and procedures will have a positive impact on both attitudes towards those policies and procedures and employee behavior.

Conclusion

Non-profits that rely on technology to help fulfill their missions face the constant risk of cyber-attacks from criminals, 'hacktivists' and insiders, whose aims are to steal, compromise or prevent access to their information (Goldernberg, 2013). While non-profits and their technology teams may be able to place a multitude of technical security features around their organizations' networks and data systems, these safeguards alone cannot ensure 100% protection from cyber-threats, regardless of the strength or advanced technical security features (Parsons, McCormac, Butavicius, Pattinson, & Jerram, 2014). Unfortunately, uneducated users (employees) will always be the most vulnerable aspect in an organization's information security platform (Imboden, Phillips, Seib, & Fiorentino, 2013). Despite the ever-increasing cyber-threats, some non-profit leaders and employees feel their organizations may be too small or that their information assets are not valuable enough for cyber criminals to attack, and therefore view their organizations' information assets as safe enough with existing technical safeguards (Zackal, 2014).

As non-profits continue to utilize technology to spur growth, cyber-threats will continue to increase and unaware and under-informed employees will continue to be a cyber-criminal's best target to gain access into an organization's data assets (Thomas, 2014). As presented, the types of inlets cyber-criminals are exploiting via the employee, at all levels, include social engineering tactics, phishing emails, mobile application malware and weak password practices

(Abawajy, 2014). These tactics all rely on user interaction to download malicious software or to obtain and compromise network login credentials (Abawajy, 2014).

In order to decrease the risk of cyber-attacks, it is imperative to build a cyber-aware workforce by developing a thorough understanding of the cyber threats facing non-profits and how best to address these threats. Therefore, it is important to identify the stakeholders who have the influence to implement the resulting mitigation strategies (Gardner, 2014). For non-profits, the stakeholders for cybersecurity initiatives may include any of the following top management positions: CIOs, technology managers, CEOs, boards of directors, risk or legal managers, and financial directors. Without the support and buy-in of these positions, any implementation or furthering of cybersecurity initiatives may fail (Gardner, 2014).

Due to the unremitting threat of breaches to an organization's cybersecurity efforts, it is imperative for an organization to invest in cyber-awareness programs just as they would invest in cybersecurity software and hardware as essential pieces of the organization's security infrastructure (Kolb & Abdullah, 2009). Not only will cyber-awareness programs help an organization to remain more secure, but they also help the organization to comply with developing information security laws (Nili, 2014). When developing effective, behavior-changing cyber-awareness programs, non-profit organizations should consider the following concepts:

(a) Understand employees' current views and perceptions around cyber security policies and procedures (Parsons et al., 2014).

(b) Understand employees' learning preferences (Clarke & Furnell, 2012).

(c) Understand the benefits and drawbacks of reward and punishment systems (Chen, Ramamurthy, & Wen, 2012).

After identifying the risks, obtaining stakeholder support and determining employee perceptions as they relate to technology security policies and their learning preferences, an organization may then consider specific types of employee training designed to address cybersecurity concerns. Cybersecurity training offerings include: (a) conventional, (b) instructor-led, (c) online, (d) game based, (e) video based, or (f) simulation based delivery-training models (Abawajy, 2014). Each training model has its potential benefits and drawbacks; however, if possible, it is best to provide multiple delivery channels as this approach will provide employees with a clearer understanding of security issues (Abawajy, 2014).

Along with identifying delivery channels, organizations should also consider the training cycle. If budgets are restrictive, a bi-annual training cycle is suggested as the absolute minimum to ensure continuing cybersecurity (Gardner, 2014). These trainings should include critical topics to the organization's security and an overview of the organization's security policies. The purpose of biannual training is to reinforce the fundamentals without detailing each security policy (Gardner, 2014). Continuous training is also considered an alternative training approach for organizations with limited budgets and may include informational posters that highlight security issues, digital newsletters that provide safety tips and how-tos, as well as lunch and learn sessions (Gardner, 2014).

An organization should determine the specific content it wishes to provide its employees with regard to cybersecurity training, as each organization may have different security issues on which to focus (Gardner, 2014). However, it is suggested that at a minimum employees should learn the three security objectives developed by the Federal Information Processing Standards Publication 199, Standards for Security Categorization of Federal Information and Information Systems, which are confidentiality, integrity and availability. These objectives help to provide a

better mental model for users to understand and effectively adapt their cybersecurity behaviors (Furman, Theofanos, Choong, & Stanton, 2012).

This annotated bibliography provides sources for examples of common cyber-risks to help refute any perceptions that non-profits are immune to cyber-threats, and highlights how employees put their organizations at risk for cyber-attacks. Relevant topics include:

- Security risks
- The importance of top-management buy-in and support
- Employee perceptions of technology security policies
- Employee learning preferences
- Training models

By understanding these key concepts, a non-profit organization will have a solid foundation for the development of a cyber-awareness program.

References

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, *33*, 237-248. http://dx.doi.org/10.1080/0144929X.2012.708787

Abraham, S., & Chengalur-Smith, I. (2010, August). An overview of social engineering malware: Trends, tactics, and implications. *Technology in Society*, *32*, 183-196. http://dx.doi.org/10.1016/j.techsoc.2010.07.001

Armerding, T. (2013). Why business is losing the war against cybercrime. Retrieved from http://www.csoonline.com/article/2133644/privacy/why-business-is-losing-the-war-against-cybercrime.html

Athitakis, M. (2014). Data security: Keep a lid on it. Retrieved from http://associationsnow.com/2014/06/data-security-keep-lid/

Basu, E. (2014, June 15). Target CEO fired - can you be fired if your company is hacked. *Forbes*. Retrieved from http://www.forbes.com/sites/ericbasu/2014/06/15/target-ceo-fired-can-you-be-fired-if-your-company-is-hacked/

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

Bissell, K. (2013, March). A strategic approach to cybersecurity. *Financial Executive*, *29*(2), 36-41. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=85919964&site=ehost-live&scope=site

Blue, V. (2014). Hacked: The six most common ways non-tech people fall victim. Retrieved from http://www.zdnet.com/hacked-the-six-most-common-ways-non-tech-people-fall-victim_p7-7000034743/#photo

Brodie, C. (2009). *The importance of security awareness training* [White paper]. Retrieved from SANS Institute website: http://www.sans.org/reading-room/whitepapers/awareness/importance-security-awareness-training-33013

Caldwell, T. (2013, February 12). Risky business: Why security awareness is crucial for employees [Blog post]. Retrieved from http://www.theguardian.com/media-network/media-network-blog/2013/feb/12/business-cyber-security-risks-employees

California data breach report [Issue brief]. (2014). Retrieved from http://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/2014data_breach_rpt.pdf?

Chen, Y., Ramamurthy, K., & Wen, K. (2012, Winter). Organizations' information security policy compliance: Stick or carrot approach? *Journal of Management Information Systems*, *29*(3), 157-188. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=cph&AN=85985309&login.asp&site=ehost-live&scope=site

Choo, K. (2011, November). The cyber threat landscape: Challenges and future research directions. *Computers & Security*, *30*, 719-731. http://dx.doi.org/10.1016/j.cose.2011.08.004

Clarke, N., & Furnell, S. (2012). Creating a security culture development plan and a case study. In O. Olivos (Ed.), *Proceedings of the sixth international symposium on human aspects of information security & assurance HAISA* 2012. HAISA (pp. 13-32). Retrieved from http://www.cscan.org/default.asp?page=openaccess&eid=13&id=28

Cohen, R. (2013). Website data breach at Maine nonprofit exposes donor info. Retrieved from https://nonprofitquarterly.org/management/21773-website-data-breach-at-maine-nonprofit-exposes-donor-info.html

Data Security and Breach Notification Act of 2014, S. S.1976, 113th Cong. (2014).

Devaney, T., & Stein, T. (2012). 5 ways small businesses can protect against cybercrime. Retrieved from http://www.forbes.com/sites/capitalonespark/2012/12/17/5-ways-small-businesses-can-protect-against-cybercrime/

Donohue, B. (2014). What is malvertising. Retrieved from http://blog.kaspersky.com/what-is-malvertising/

Epstein, A. J. (2014, September/October). Thinking strategically about cyber risk. *NACD Directorship*, 32-35. Retrieved from http://thirdcreekadvisors.com/wp/wp-content/uploads/2014/09/Ridge-Interview-Directorship.pdf

Furman, S. M., Theofanos, M. F., Choong, Y., & Stanton, B. (2012, March/April). Basing cybersecurity training on user perceptions. *IEEE Security & Privacy*, *10*(2), 40-49. http://dx.doi.org/10.1109/MSP.2011.180

Gardner, B. (2014). Who is responsible for security. In B. Gardner, & V. Thomas, *Building an information security awareness program defending against social engineering and technical threats* (1st ed. (Loc. 1184-1304). [Kindle]. Retrieved from Amazon.com

Gardner, B., & Thomas, V. (2014). *Building an information security awareness program Defending against social engineering and technical threats* (1st ed.). Retrieved from http://www.amazon.com

Goldernberg, P. (2013). The cyber threat to non-governmental organizations. Retrieved from https://ctovision.com/2013/10/cyber-threat-non-governmental-organizations/

Grawemeyer, B., & Johnson, H. (2011). Using and managing multiple passwords: A week to a view. *Interacting with Computers*, *23*, 256-267. http://dx.doi.org/doi:10.1016/j.intcom.2011.03.007

Guttman, B., & Roback, E. (1995, October). Special publication 800-12: An introduction to computer security: The NIST handbook. *NIST Special Publication*, 3-269. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf

Harris, K. D. (2014). *California data breach report*. Retrieved from http://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/2014data_breach_rpt.pdf?

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012, August). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences Journal*, *43*, 615-659. http://dx.doi.org/10.1111/j.1540-5915.2012.00361.x

Imboden, T. R., Phillips, J. N., Seib, J., & Fiorentino, S. R. (2013). How are nonprofit organizations influenced to create and adopt information security policies. *Issues in Information Systems*, *14*, 166-173. Retrieved from http://iacis.org/iis/2013/269_iis_2013_166-173.pdf

Kolb, N., & Abdullah, F. (2009). Developing an information security awareness program for a non-profit organization. *International Management Review, 5*, 103-107. Retrieved from http://web.b.ebscohost.com/

Majority of U.S. small businesses say digital literacy essential skillset for new hires. (n.d.). Retrieved from http://www.staysafeonline.org/about-us/news/majority-of-united-states-small-businesses-say-digital-literacy-essential-skillset-for-new-hires

Nili, Y. (2014, August 25). Understanding and implementing the NIST cybersecurity framework [Online forum comment]. Retrieved from http://blogs.law.harvard.edu/corpgov/2014/08/25/understanding-and-implementing-the-nist-cybersecurity-framework/

Paganini, P. (2013). 2013 - the impact of cybercrime. Retrieved from http://resources.infosecinstitute.com/2013-impact-cybercrime/

Parker, K. (2014, September 9). Hack attacks: Headed your way [Blog post]. Retrieved from http://aaronwolowiec.com/tag/cyber-attack/

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014, May). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Computers & Security*, *42*, 165-176. http://dx.doi.org/10.1016/j.cose.2013.12.003

Ponemon Institute. (2014). *2014 cost of data breach study: United States*. Retrieved from http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&appname=GTSE_SE_SE_USEN&htmlfid=SEL03017USEN&attachment=SEL03017USEN.PDF#loaded

Posthumus, S., & von Solms, R. (2004, October 27). A framework for the governance of information security. *Computers & Security*, *23*, 638-646. http://dx.doi.org/10.1016/j.cose.2004.10.006

Rai, S. (2014). *Cybersecurity what the board of directors need to ask*. Retrieved from https://na.theiia.org/special-promotion/PublicDocuments/GRC-Cybersecurity-Research-Report.pdf

Ranger, S. (2014). Average company now compromised every four days, with no end to the cybercrime wave in sight. Retrieved from http://www.zdnet.com/average-company-now-attacked-every-four-days-with-no-end-to-the-cybercrime-wave-in-sight-7000034755/

Renaud, K., & Goucher, W. (2014). The curious incidence of security breaches by knowledgeable employees and the pivotal role a of security culture. In T. Tryfonas, & I.

Askoxylakis, *Human aspects of information security, privacy, and trust* (pp. 361--372). http://dx.doi.org/10.1007/978-3-319-07620-1_32

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L., & Downs, J. (2010). *Who falls for phish?: A demographic analysis of phishing susceptibility and effectiveness of interventions*. Paper presented at the Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, New York, NY. Abstract retrieved from http://doi.acm.org/10.1145/1753326.1753383

Symantec Corporation. (2014). *Internet security threat report 2014*. Retrieved from Symantec website: http://www.symantec.com/security_response/publications/threatreport.jsp

Thomas, V. (2014). Social engineering. In B. Gardner, & V. Thomas, *Building an information security awareness program* (1st ed. (1489). Retrieved from www.amazon.com

Zackal, J. (2014). Cyber security q&a: Nonprofits at risk. Retrieved from http://thirdsectortoday.com/2014/07/30/ cyber-security-qa-nonprofits-at-risk/