Online Journal of Applied Knowledge Management

A Publication of the International Institute for Applied Knowledge Management

Volume 6, Issue 1, 2018

Expert assessment of organizational cybersecurity programs and development of vignettes to measure cybersecurity countermeasures awareness

Jodi Goode, Nova Southeastern University, USA, jp1587@mynsu.nova.edu

Yair Levy, Nova Southeastern University, USA, levyy@nova.edu

Anat Hovav, Korea University Business School, South Korea, anatzh@korea.ac.kr

James Smith, Augusta University, USA, jasmith8@augusta.edu

Abstract

As organizational reliance on technology increases, cybersecurity attacks become more attractive to attackers and increasingly devastating to organizations. Due to lacking knowledge and skills, humans are often considered the most susceptible threat vector for cyber attacks. Previous studies in information systems (IS) literature have confirmed awareness techniques to be the first step in increasing employee cybersecurity-related knowledge, promoting security-conscious decision-making, and the prevention of naive IS security behaviors. While training initiatives exist within many organizations, there appears to be a limited number of empirical research studies that focus on what security education, training, and awareness (SETA) programs should encompass. This includes topics to be covered, the most valuable method for delivery, and to what degree these factors play a part in the IS security practice of employees. The aim of this study was to use subject-matter experts (SMEs) to validate: 1) the key topics needed for two SETA program types (typical & socio-technical), 2) the measurement criteria for employees' cybersecurity countermeasures awareness (CCA), 3) weights for the three CCA categories (awareness of policy, SETA, & monitoring) in the overall CCA measure, and 4) two SETA programs content with integrated vignette-based assessments for CCA. A Delphi methodology was utilized to gather feedback from 21 SMEs regarding cybersecurity topics for organizational SETA programs, validation of SETA training content, and to develop a vignette-based measure of CCA. Results show that awareness of the organizational cybersecurity policy was the most important category for the overall CCA measure with 41%, followed by awareness of SETA program content, with 34%, while awareness of monitoring was 25%. The paper concludes with discussions and future research agenda.

Keywords: Cybersecurity; cybersecurity skills; cybersecurity countermeasures awareness; security; security education, training, and awareness (SETA).

Introduction

The protection of an organization's information systems (IS) and information assets from cybersecurity threats is increasingly important in today's world, especially as businesses become more reliant upon technology for daily business processes (D'Arcy, Hovav, & Galletta, 2009).

Companies in the United States continue to lead the world in losses from cyber attacks, with 58 organizations reporting the mean cost per organization for 2015 as $12.7 million (Ponemon Institute, 2015). Employees who lack knowledge and skillsets are seen as a susceptible threat vector for cyber attacks, and therefore, are being targeted with continually evolving threats (Jang-Jaccard & Nepal, 2014). A study of 252 global organizations found nine key cyber attack vectors, most of which focused on the human factor in information security including viruses, malware, Web-based attacks, phishing and social engineering, malicious code, denial of services, as well as stolen devices (Ponemon Institute, 2015). However, organizations that have established an effective technical layer of information security continue to experience difficulties triggered by cybersecurity threats. Ultimately, the cybersecurity posture of an organization depends on appropriate actions taken by employees, who are often cited as the weakest link in IS security domain (Al-Omari, El-Gayar, & Deokar, 2012; Albrechtsen, 2007; Rhee, Kim, & Ryu, 2009).

According to Furnell et al. (1996), the need to promote IS security policy and awareness within the organization requires first the establishment of valid IS security awareness training. Employees' lack of awareness of threats posed in the cyber realm increases the susceptibility of malicious attacks and organizational losses (Shaw, Chen, Harris, & Huang, 2009). While training initiatives exist within many organizations, there appears to be a limited number of empirical research studies to determine what topics should be covered, the most valuable method used for delivery, and to what degree these factors play a part in the IS security practice of employees. Consequently, for the training program to be considered effective, cybersecurity countermeasures awareness (CCA) must be measured and improvements made. However, challenges for the determination of security education, training, and awareness (SETA) program outcomes competency are posed by the existing measures of CCA, which are dated and limited. Development and validation of a measurement tool to properly assess the CCA level of employees was imperative due to the limitations of construct measurement in previous research, while self-assessment instruments are known to provide inaccurate measures. In this first phase of the larger research study, a panel of subject matter experts (SMEs) addressed four specific research questions:

RQ1: What are the SMEs' approved topics for the two SETA program types (typical & socio-technical)?

RQ2: What are the SMEs' approved measurement criteria for CCA?

RQ3: What are the SMEs' approved weights for the three CCA categories (awareness of policy, SETA, & monitoring)?

RQ4: What are the SMEs' approved two SETA program types (typical & socio-technical) content?

The Delphi methodology was used to determine SMEs' approved topics for organizational SETA programs, measurement criteria for CCA through review and feedback on vignettes drafted based on previous research, the weights of the three CCA categories, as well as the validation of content for two SETA program types (typical & socio-technical).

Literature Review

Cybersecurity Threats

Approximately 72% to 95% of the cybersecurity threats and vulnerabilities for organizations have been linked to the naive cybersecurity practices of employees or contractors (D'Arcy et al., 2009; IBM Global Technology Services, 2014). Of these, most security incidents are attributed to current or former employees of the organization (PricewaterhouseCoopers, 2016). IBM Global Technology Services (2014) found the most prevalent practice to be unsafe Web browsing, which can lead to IS compromise via malware. Malware is the leading tool used by cyber-attackers to carry out malicious acts and is known to advance rapidly to capitalize on new approaches to exploit flaws in emerging technologies (Jang-Jaccard & Nepal, 2014). Furthermore, social engineering attacks are on the rise and are considered the greatest security threat to people and organizations (Algarni, Xu, Chan, & Tian, 2014). Even the most technologically advanced IS security measures can be thwarted by social engineering, which utilizes tactics to trick victims into compromising personal or organizational security defenses through phishing, vishing (voice solicitations), and impersonation (Algarni et al., 2014). While employee awareness of social engineering techniques is important, Kvedar, Nettis, and Fulton (2010) found that even those who classify themselves as aware of these tactics can be fooled. Likewise, an employee with IS knowledge does not necessarily possess the cybersecurity skills required to protect themselves and their organization from cyber threats (Choi, Levy, & Hovav, 2013). Therefore, expanding knowledge of both countermeasures awareness and skills, as well as SETA program type and delivery method are significant not only to add to the body of knowledge in relation to cybersecurity, but also for practitioners who are charged with protecting organizational IS and information assets.

Cybersecurity Countermeasures Awareness

Awareness is defined as the extent to which a specific population is cognizant of an innovation and formulates a general perception of what it involves (Dinev & Hu, 2007). The organizational impact from awareness strategies have long been studied in social science, criminal justice, as well as medical behavioral sciences and positively linked to individuals' cognitive development (Shaw et al., 2009). For awareness to be achieved, an organization or individual must be exposed to the existence of the innovation, while providing information on both how it functions and what its benefits are. Awareness of the significance of cybersecurity, personal responsibility in protecting organizational data, as well as of recent advances by those with malicious intent is imperative given the level of organizational concern today regarding emerging cybersecurity threats (Shaw et al., 2009).

Straub and Welke (1998) used the term security countermeasures to collectively describe a mix of procedural and technical controls to mitigate IS security risks. Building upon previously used security countermeasures definitions, CCA can be said to include employee awareness of security policies, SETA programs, computer monitoring, and computer sanctions (Choi et al., 2013; D'Arcy et al., 2009). CCA can also be described as the state where individuals are aware of their cybersecurity mission within the organization (Katz, 2005; Rezgui & Marks, 2008). Previous studies related to deterrence of naive IS security behavior had found positive influence

of various security countermeasures (Kankanhalli, Teo, Tan, & Wei, 2003; Lee & Lee, 2002). D'Arcy et al. (2009) extended prior work by focusing on the impact of user awareness of security countermeasures on IS misuse intention. The underlying process through which the security countermeasures of security policy, SETA program, and computer monitoring impacted naive behaviors was explored. However, additional research on countermeasures awareness that specifically focuses on cybersecurity threats is needed to determine the most effective method for organizations to address issues from a human-centric lens.

Security Education, Training, and Awareness (SETA) Programs

Stanton, Stam, Mastrangelo, and Jolton (2005) stated that even the best technology efforts intended to address IS security will fail unless the organization's employees take the proper course of action when approached with a cyber threat. Although technology-oriented safeguards such as firewalls, intrusion detection systems (IDS), and intrusion prevention systems (ITS) are found in a large number of organizations, focus on human factors in cybersecurity, including awareness and skills development training initiatives, have historically lagged behind (Carlton & Levy, 2015; Furnell & Clarke, 2012). SETA programs take many forms, but quality programs raise employee awareness of responsibilities in relation to their organizations' information assets, provide instruction on the consequences of abuse, and develop the necessary foundational cybersecurity skills to help fulfill these requirements (Carlton & Levy, 2015; D'Arcy & Hovav, 2007; Whitman, Townsend, & Alberts, 2001). Regardless of the form, the organizational IS security policy should provide the foundation of the SETA program. Many typical SETA programs seem to focus on memorization and often involve coercion, fear tactics, or perception of external pressures, which have been found to have no influence on employee compliance with organizational IS policies (Kranz & Haeussinger, 2014; Parrish & Nicolas-Rocca, 2012). However, according to Parsons, McCormac, Butavicius, Pattinson, and Jerram (2014), training and education efforts are more effective if they not only outline what is expected but also provide an understanding of why this is important to the individual or employee, often called socio-technical philosophies. For this reason, socio-technical philosophies are understood to be more valuable, providing a means for employees to easily see how the training materials used can correlate to their day-to-day duties (Netteland, Wasson, & Morch, 2007). Socio-technical philosophies embrace social as well as technical elements for optimal design and use of organizational systems (Davis, Challenger, Jayewardene, & Clegg, 2014). Furthermore, it is imperative that the most effective delivery method for the specific program type be empirically investigated (Paul, 2014). Both online and face-to-face training delivery methods have their advantages, and in previous research, each has been found to successfully produce a motivated employee who has the skills needed to apply their training to job-related tasks (Gupta, Bostrom, & Huber, 2010). However, there seems to be insufficient research in the field of IS to determine the most successful delivery method as well as the type of program for cybersecurity-focused SETA programs.

Methodology

The Delphi methodology has been proven to provide both validity and reliability in situations when there is no source of factual data but a basis for opinion exists (Gray & Hovav, 2008;

Ramim & Lichvar, 2014). It was designed to encourage true SME debate through the use of techniques, which allow for anonymity, iteration, and controlled feedback (Gordon & Glenn, 2009). Techniques seek to expose the measures to SMEs who often have differing opinions, effectively utilizing a group communication process to refine the measures based on the consensus building input of the SME panel (Ramim & Lichvar, 2014).

According to Clayton (1997), the panel size can vary depending on the complexity and the expertise required for consensus on the topic. Best practice for homogeneous populations, such as cybersecurity SMEs, is a panel of 15 to 30 professionals with diverse backgrounds and expertise within the field, as well as varying in age and education (Clayton, 1997). Consensus for Delphi studies typically ranges from 55% to 100% agreement, with 70% considered the standard (Vernon, 2009). Thus, this study employed the Delphi methodology, where SMEs from the cybersecurity discipline were identified and asked to participate in the research. Qualitative methods are often used to discover evidence, and will require the assistance of SMEs per the Delphi methodology to determine the topics to be covered in the SETA program, to validate and refine the measure of CCA, and to approve the content of the two SETA programs with integrated vignette-based assessments for CCA (See Figure 1).

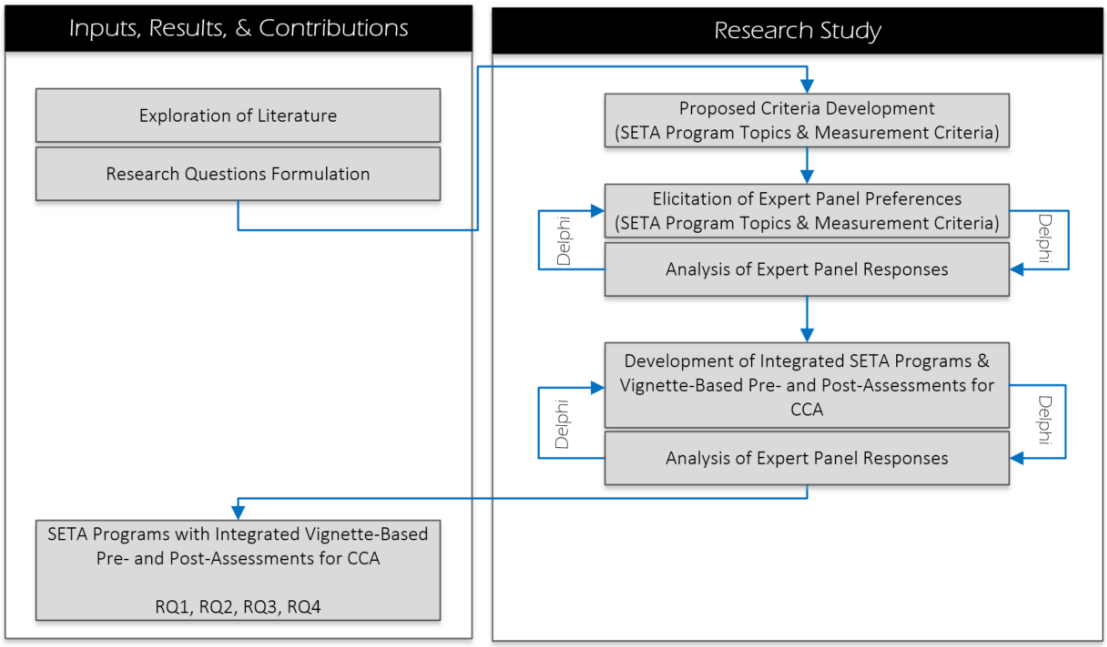

Figure 1: Overview of this study's research methodology process

Data Analysis and Results

A panel of 38 experts was targeted with 21 responding in each of the two Delphi rounds, representing 55.2% response rate (See Table 1 for panel descriptive statistics). Engaging those with skillsets and expertise in the area of study, cybersecurity in this research, allowed the group to confirm that the measures are adequate and fully representative of the concepts (Sekaran &

Bougie, 2013). Agreement percentages ranged from 85% to 100% for questions asked of the panel, which is well above what the standard for consensus in Delphi studies.

Consistent with recommendations from Gordon and Glenn (2009) as well as Ramim and Lichvar, (2014), once SMEs agreed to participate, instrument questions were refined and pursued through two sequential Delphi rounds delivered via anonymous Web-based method. In round one, SMEs were asked to provide their judgment as well as feedback on a) SETA program topics, b) the CCA vignette-based assessment, and c) weights for the three CCA categories (awareness of policy, SETA, & monitoring). Given the very high agreement among the SMEs on the instrument questions, no additional cycles were needed for round one. In round two, SMEs reviewed the SETA program content for both the typical and socio-technical courses to provide validation. For each of these items, SME feedback was analyzed and synthesized to determine that a clear consensus on each topic was provided with no need to proceed with follow-up rounds.

Table 1. Descriptive Statistics of SMEs (N=21)

Demographic Item	Frequency	Percentage
Gender:		
Female	6	28.6%
Male	15	71.4%
Current Employment:		
Academia	6	28.6%
Industry	5	23.8%
Both	10	47.6%
Age:		
20-29 years	1	4.8%
30-39 years	6	28.6%
40-49 years	9	42.9%
50-59 years	5	23.8%
Experience in Information Systems and/or Cybersecurity:		
1-5 years	0	0%
6-10 years	2	9.5%
11-15 years	8	38.1%
16-20 years	4	19.0%
20 years or more	7	33.3%
Cybersecurity Certifications:		
0	5	23.8%
1	7	33.3%
2	5	23.8%
3 or more	4	19.0%

SETA Program Topics

According to D'Arcy and Hovav (2007), SETA program topics should be based upon the security policy of the organization. Key foundational topics are required for any common program to ensure its effectiveness; however, this assertion has not been empirically validated. As a baseline, in round one, SMEs were asked to validate a list of relevant cybersecurity topics based on suggestions in ISO/IEC 27002 standards for IS security policy (ISO/IEC, 2013). SMEs indicated whether the topic was one that should be included in a common organizational SETA program, provided revision of topics when needed, and were encouraged to suggest any additional topics that should be covered in nowadays' organizational environments. While the experts deemed most of the ISO/IEC 27002 topic suggestions important, the subjects of cryptographic controls and vendor relationships were found to be irrelevant for many organizations. Based on SMEs' feedback, Table 2 provides a list of the topics and subtopics that were determined to be the key foundational ones for inclusion in organizational SETA programs.

Table 2. Key Foundational SETA Programs Topic

Data Security	**Common Risks & Vulnerabilities**	**Accessing Work Systems**
Data classification & acceptable use	Spam	Mobile security
Privacy	Phishing and vishing	Working remotely
Personally identifiable information (PII)	Safe browsing	Bring Your Own Device (BYOD)
Physical and environmental security	Malware	Cloud
Data backup and storage	Ransomware	
Data encryption and destruction	Social Engineering	**Password Management**
Data loss (accidental vs. malicious)	Advanced persistent threats (APT)	Creating strong passwords
Data regulations – FERPA, HIPAA, PCI, etc.	Software restrictions (use and copyright)	Password security

Cybersecurity Countermeasures Awareness (CCA) Measure

The measurement instrument for CCA was developed based on the security countermeasures assessments of Hovav and D'Arcy (2012) as well as Vance, Siponen, and Pahnila (2012). Although previous work presented these items in survey format, this study novelty as it utilized a vignette-based assessment of CCA (See Figure 2 for a sample of one of the vignettes). The vignettes cover awareness of policy, SETA, as well as monitoring and address key, IS security policy topics (Doherty, Anastasakis, & Fulford, 2011; SANS Institute, 2014). In round one, the Delphi methodology was used to obtain SMEs feedback on several key aspects of the adapted vignettes. A total of nine vignettes were drafted, with three for each of the three CCA categories based on previous empirically validated research studies (D'Arcy et al., 2009; Hovav & D'Arcy, 2012; Vance et al., 2012). SMEs were asked to review the vignettes to ensure 1) clarity of wording, 2) validity in the context of the policy topic, 3) that the actions provided address the possible outcomes of the vignettes, 4) that the actions measure the cybersecurity countermeasures awareness of the three categories (awareness of policy, SETA, & monitoring) of the individual, and 5) that the scores were assigned appropriately. Based on the feedback from the 21 SMEs, minor adjustments were made to clarify vignettes' wording, to better address possible actions, and to ensure accurate scoring.

Sandy's supervisor requests her to leave the office computer unlocked so that other employees can use it while she is out to lunch or away from the office. Sandy should:

Option	Action	Score
A	Leave her computer unlocked as requested by her supervisor.	0
B	Leave her computer unlocked as requested by her supervisor and report this incident to IT/IT Security.	4
C	Continue to lock her computer and inform her supervisor that the request goes against the organization's acceptable use policy.	8
D	Continue to lock her computer, inform her supervisor that the request goes against the organization's acceptable use policy, and report this concern to IT/IT Security.	10

Figure 2. Example of one of the CCA vignettes for the awareness of policy category

In addition to validating key aspects of the CCA vignettes, SMEs were also asked to provide their feedback on the weight of each of the three categories (awareness of policy, SETA, & monitoring), with the sum of the three totaling 100%. Answers across all 21 SMEs were averaged to calculate the weight for each category. Figure 3 shows the weights of the three CCA categories with standard deviation.

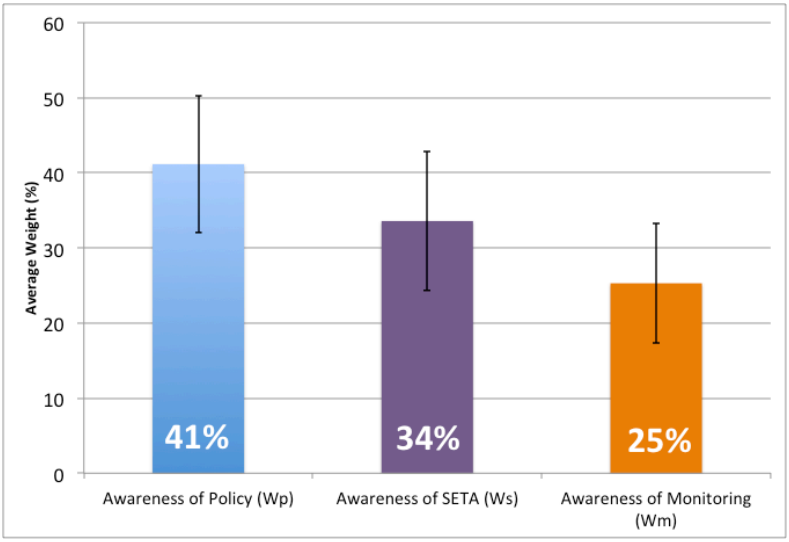

Figure 3. Weights of the three CCA categories with standard deviation

Results indicated that the most important category for the overall CCA measure was awareness of the organizational cybersecurity policy, with 41%. The second most important category for the overall CCA measure was awareness of SETA program content, with 34%, while awareness of monitoring provided the least importance among the three with 25% (See Figure 4). The SMEs validation of the CCA vignettes and the percentages for each of the three categories provided an empirically validated vignette-based assessment of CCA to be integrated into the SETA program as both the pre- and post-assessments.

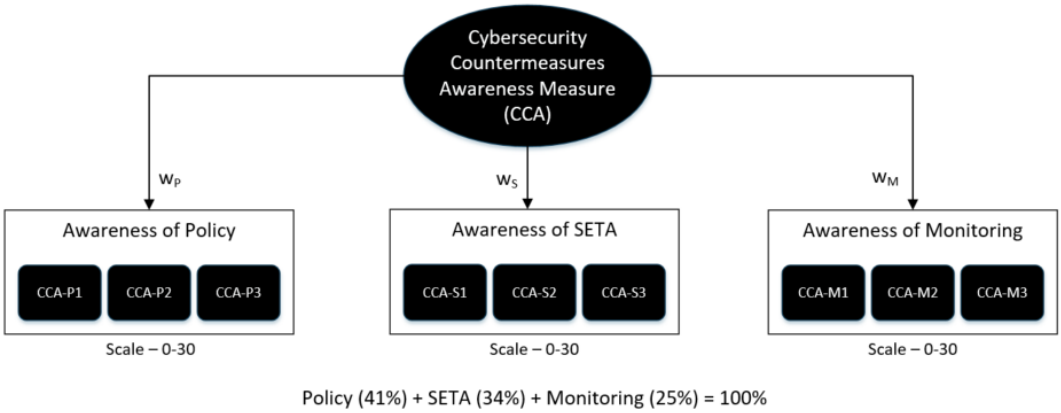

Figure 4. Research design for weights of the three CCA categories

SETA Program Content

In a future phase of this research study, an organizational SETA program will be delivered in two types: typical program and socio-technical program. Given the focus of our study on typical vs. socio-technical program types, it was critical that expert opinion of both types of content be confirmed before moving forward. It was explained to the SMEs that the typical SETA program should inform the employee of organizational policies and actions that should or should not be taken, while the socio-technical SETA program should also include explanations of why certain actions may cause difficulties as well as the potential organizational outcomes associated.

Table 3. SETA program content

		Content Items
Program Type	Typical SETA	Reading material
		Lectures from cybersecurity expert
		Videos from SANS Institute & KnowBe4
	Socio-Technical SETA	Reading material delivered via LMS
		Lectures from cybersecurity expert
		Videos from SANS Institute & KnowBe4
		Why is this important? How does it relate to my daily job duties?

Delphi round two of this study focused on SME validation of the SETA program content that later will be used in the future phase of the research study. The cybersecurity topics determined important by SMEs in round one for delivery were utilized and content created for the two program types (typical & socio-technical). This content included reading material, lectures from an expert in the field of cybersecurity, and topic appropriate videos from the SANS Institute and KnowBe4 training curriculums (See Table 3). SMEs were provided with the opportunity to

review material for five of the cybersecurity topics as a representation of the comprehensive content developed. They were asked to 1) verify that the typical training content was what they would expect of an organizational SETA program, 2) to determine if the socio-technical content additions provided the participant with more information on why the content is important to them personally and identification of how the training materials can correlate to their day-to-day duties, and 3) to provide any additional feedback or revision suggestions.

Conclusion and Discussion

The main goal of this research study was to determine expert-approved topics for the two SETA program types (typical & socio-technical), vignettes for measuring CCA, weights for the three CCA categories (awareness of policy, SETA, & monitoring), as well as SETA program content for both the typical and socio-technical program types. Per best practice, Delphi measures were administered, precise questions were used, assurance of anonymity was provided to the SMEs to ensure they were not influenced by the responses of others, and consensus was reached to answer each of the four research questions (Gray & Hovav, 2008).

Future Research

D'Arcy et al. (2009) established that implementation of a SETA program is critical to the mitigation of cybersecurity threats within an organization. Prior studies have touted the need for SETA but very few have focused on what SETA should encompass and the factors that are likely to increase success. The development of CCA through SETA initiatives is imperative; however, additional research is needed to determine the most valuable program type and delivery method, i.e. online vs. face-to-face. Therefore, this was the first phase of a larger research study that aims to empirically assess if there are any significant differences on employees' CCA and cybersecurity skills (CyS) based on the use of two SETA program types (typical vs. socio-technical) and two SETA delivery methods (face-to-face & online).

References

Al-Omari, A., El-Gayar, O., & Deokar, A. (2012). Security policy compliance: User acceptance perspective. *Proceedings of the 45th Hawaii International Conference on System Science*, 199-216.

Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers & Security, 26*(4), 276-289.

Algarni, A., Xu, Y., Chan, T., & Tian, Y.-C. (2014). Social engineering in social networking sites: How good becomes evil. *Proceedings of the Pacific Asia Conference on Information Systems*, 1-10.

Carlton, M., & Levy, Y. (2015). Expert assessment of the top platform independent cybersecurity skills of non-IT professionals. *Proceedings of the IEEE SoutheastCon Conference*, 1-6. doi:10.1109/SECON.2015.7132932.

Choi, M. S., Levy, Y., & Hovav, A. (2013). The role of user computer self-efficacy, cybersecurity countermeasures awareness, and cybersecurity skills influence on computer misuse. *Proceedings of the Pre-International Conference of Information Systems on Information Security & Privacy*, 1-19.

Clayton, M. J. (1997). Delphi: A technique to harness expert opinion for critical decision making tasks in education. *Educational Psychology, 17*(4), 373-386.

D'Arcy, J., & Hovav, A. (2007). Deterring internal information systems misuse. *Communications of the ACM, 50*(10), 113-117.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research, 20*(1), 79-98.

Davis, M. C., Challenger, R., Jayewardene, D. N., & Clegg, C. W. (2014). Advancing socio-technical systems thinking: A call for bravery. *Applied Ergonomics, 45*(2), 171-180.

Dinev, T., & Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *Journal of the Association for Information Systems, 8*(7), 23.

Doherty, N. F., Anastasakis, L., & Fulford, H. (2011). Reinforcing the security of corporate information resources: A critical review of the role of the acceptable use policy. *International Journal of Information Management, 31*(3), 201-209.

Furnell, S., & Clarke, N. (2012). Power to the people? The evolving recognition of human aspects of security. *Computers & Security, 31*(1), 983-988.

Gordon, T., & Glenn, J. (2009). *Futures research methodology*.

Gray, P., & Hovav, A. (2008). From hindsight to foresight: Applying futures research techniques in information systems. *Communications of the Association for Information Systems, 22*(1), 12.

Gupta, S., Bostrom, R. P., & Huber, M. (2010). End-user training methods: What we know, need to know. *Communications of the ACM, 41*(4), 9-39.

Hovav, A., & D'Arcy, J. (2012). Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the US and South Korea. *Information & Management, 49*(2), 99-110.

IBM Global Technology Services. (2014). IBM security services 2014 cybersecurity intelligence index. Retrieved from http://www-03.ibm.com/security/services/2014-cyber-security-intelligence-index-infographic/

ISO/IEC. (2013). ISO/IEC 27002. *2013 Information technology- Security techniques - Code of practice for information security controls.* Retrieved from https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-2:v1:en

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer & System Sciences, 80*(5), 973-993.

Kankanhalli, A., Teo, H.-H., Tan, B. C., & Wei, K.-K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management, 23*(2), 139-154.

Katz, F. H. (2005). The effect of a university information security survey on instruction methods in information security. *Communications of the ACM, 34*(2), 43-48.

Kranz, J., & Haeussinger, F. (2014). Why deterrence is not enough: The role of endogenous motivations on employees' information security behavior. *International Conference on Information Systems*, Auckland, Australia.

Kvedar, D., Nettis, M., & Fulton, S. P. (2010). The use of formal social engineering techniques to identify weaknesses during a computer vulnerability competition. *Journal of Computing Sciences in Colleges, 26*(2), 80-87.

Lee, J., & Lee, Y. (2002). A holistic model of computer abuse within organizations. *Information Management & Computer Security, 10*(2), 57-63.

Netteland, G., Wasson, B., & Morch, A. I. (2007). E-learning in a large organization: A study of the critical role of information sharing. *Journal of Workplace Learning, 19*(6), 392-411.

Parrish, J. L., & Nicolas-Rocca, S. (2012). Toward better decisions with respect to is security: Integrating mindfulness into IS security training. *Pre-ICIS Workshop on Information Security & Privacy*, Orlando, FL.

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.

Paul, T. V. (2014). An evaluation of the effectiveness of e-learning, mobile learning, and instructor-led training in organizational training and development. *Journal of Human Resource & Adult Learning, 10*(2), 1-13.

Ponemon Institute. (2015). *Cost of cyber crime study.* Retrieved from http://www8.hp.com/us/en/software-solutions/ponemon-cyber-security-report/

PricewaterhouseCoopers. (2016). The global state of information security survey 2016. Retrieved from http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html

Ramim, M. M., & Lichvar, B. T. (2014). Eliciting expert panel perspective on effective collaboration in system development projects. *Journal of Applied Knowledge Management, 2*(1), 122-136.

Rezgui, Y., & Marks, A. (2008). Information security awareness in higher education: An exploratory study. *Computers & Security, 27*(7–8), 241-253.

Rhee, H. S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security, 28*(8), 816-826.

SANS Institute. (2014). *Information security policy templates*. Retrieved from https://www.sans.org/security-resources/policies/

Sekaran, U., & Bougie, R. (2013). *Research methods for business: A skill building approach*: John Wiley & Sons.

Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H.-J. (2009). The impact of information richness on information security awareness training effectiveness. *Computers & Education, 52*(1), 92-100.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & Security, 24*(2), 124-133.

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *Management Information Systems Quarterly, 22*(2), 441-470.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management, 49*(4), 190-198.

Vernon, W. (2009). The Delphi technique: A review. *International Journal of Therapy and Rehabilitation, 16*(2), 69-76.

Whitman, M. E., Townsend, A. M., & Alberts, R. J. (2001). Information systems security and the need for policy. *Information Security Management, 24*, 9-18.

Authors' Biographies

Jodi Goode, Ph.D. is Assistant Vice President for Information Technology Services, Chief Information Officer, and adjunct instructor of Computer Information Systems at Howard Payne University, Brownwood, Texas and has fifteen years of experience in the information systems and cybersecurity field. She earned a Bachelor's degree in Computer Information Systems and Master's degree in Information Systems from Tarleton State University, Stephenville, Texas. Jodi obtained her Ph.D. in Information Systems with a concentration in Information Security from Nova Southeastern University.

Yair Levy, Ph.D. is a Professor of Information Systems and Cybersecurity at the College of Engineering and Computing at Nova Southeastern University, the Director of the Center for Information Protection, Education, and Research (CIPhER) (http://infosec.nova.edu/), and chair of the Information Security Faculty Group at the college along with serving as the director of the M.S. and Ph.D. programs in Cybersecurity and Information Assurance. He heads the Levy CyLab (http://CyLab.nova.edu/), which conducts innovative research from the human-centric lens of four key research areas Cybersecurity, User-authentication, Privacy, and Skills, as well as their interconnections. Levy authored one book, three book chapters, and numerous peer-reviewed journal as well as conference proceedings publications. His scholarly research have cited over 3,100 times. Dr. Levy has been an active member of the US Secret Service (USSS)'s - Miami Electronic Crimes Task Force (MECTF) and The South Florida Cybercrime Working Group (SFCWG). He was trained by the Federal Bureau of Investigation (FBI) on various topics, and actively serves as a board member on the South Florida FBI/InfraGard, and consults federal agencies, state and local government groups on cybersecurity topics. He is also a frequent invited

keynote speaker at national and international meetings, as well as regular media interviews as a Subject Matter Expert (SME) on cybersecurity topics. Read more about Dr. Levy via: http://www.nova.edu/~levyy/

Anat Hovav, Ph.D. is a professor at Korea University Business School in Seoul, South Korea. Her research interests include the socio-technical aspects of organizational information security, risk assessment, innovation management, and Futures research. Professor Hovav has published in internationally refereed journals such as Information Systems Research (ISR), Information & Management, Communications of the ACM, Journal of Business Ethics, Research Policy, Computers & Security, Information Systems Journal (ISJ), Journal of Pervasive and Mobile Computing, International Journal of Project Management, Information Systems Management (ISM), Communications of AIS (CAIS), Information Systems Frontiers, and Risk Management and Insurance Review. Dr. Hovav is the winner of the 2013 Citation of Excellence Award. She has presented her work internationally in academic and industry conferences and workshops. Dr. Hovav is the current president of the AIS special interest group on security and privacy (SIGSEC), and has chaired a number of information security related workshops and tracks at major conferences such as ICIS, AMCIS and ECIS.

James N. Smith, DBA, CISSP is an Assistant Professor of Cybersecurity at Augusta University, USA. He is a graduate of Kennesaw State University and an alumnus of the 2015 ICIS Doctoral Consortium. James formerly served on the Board of Directors of the Southern Association of Information Systems and serves on the Board of Directors of MMI Capital, LLC.