SHRM-SIOP Science of HR Series

Implementing Effective Cyber Security Training for End Users of Computer Networks

Richard E. Beyer
rebeyer@integritas-llc.com
Integritas, LLC

Bradley J. Brummel
bradley-brummel@utulsa.edu
The University of Tulsa

SHRM
SOCIETY FOR HUMAN RESOURCE MANAGEMENT

SIOP
SOCIETY for INDUSTRIAL and ORGANIZATIONAL PSYCHOLOGY
SCIENCE FOR A SMARTER WORKPLACE

Richard Beyer recently received his M.A. in industrial and organizational psychology from The University of Tulsa and is founder and managing member of Integritas, LLC. Formerly senior vice president of human resources for NationsBank and JE Dunn Construction, he also served as Kansas Secretary of Labor. Active in the American Institute of Certified Public Accountants, the Society for Human Resource Management, the Society for Industrial and Organizational Psychology, and WorldatWork, Mr. Beyer is a Certified Public Accountant (CPA), SHRM Senior Certified Professional (SHRM-SCP), Senior Professional in Human Resources (SPHR) and a Certified Compensation Professional (CCP). He has conducted research on cyber trust and evidence-based human resource management, which has been published in the *Journal of the Colloquium for Information Systems Security Education (CISSE)* and the *Personnel Administrator*.

Bradley Brummel is an associate professor of psychology at The University of Tulsa. He received his Ph.D. in industrial and organizational psychology from the University of Illinois at Urbana-Champaign. Dr. Brummel conducts research on organizational training and development focusing on coaching and simulation-based delivery methods for professional ethics and cyber security content areas. He is a member of the Society for Industrial and Organizational Psychology, the Academy of Management and the Association for Research in Personality. Dr. Brummel's research has been published in *Personnel Psychology*, *Journal of Applied Psychology*, *Journal of Management* and *Human Relations*.

Author Note

This work was sponsored in part by the Air Force Office of Scientific Research (AFOSR), under award number FA9550-12-1-0457. Any opinions, findings and conclusions or recommendations expressed in this publication are those of the authors and do not necessarily reflect the views of the AFOSR.

Correspondence concerning this paper should be addressed to Richard E. Beyer, 2640 W. 118th Terrace, Leawood, KS 66211. E-mail: rebeyer@integritas-llc.com

ABSTRACT

Cyber security is a concern for all modern organizations. These organizations cannot achieve their cyber security goals through hardware and information technology (IT) workers alone, so all employees who use computer networks must be trained on the knowledge, skills and policies related to cyber security. This paper reviews what is known about effective cyber security training for end users of computer systems and offers suggestions about how human resource (HR) leaders can effectively implement this training. This includes a broad review of the cyber security policies and competencies that are the basis for training needs analysis, setting learning goals, and effective training design. Finally, the paper discusses opportunities for human resource (HR) practitioners, industrial and organizational (I-O) psychologists, and information technology (IT) specialists to integrate their skills and enhance the capabilities of organizations to counteract cyber security threats.

Introduction

Cyber security operations involve core technologies, processes and practices designed to protect networks, computers, programs, people and data from attack, damage, injury or unauthorized access. Given the cyber threat environment, effective systems must also involve employee end users of organizational computer systems. In fact, nearly all employees with access to computers or networks play a cyber security role in their organizations whether they know it or not.

Both cyber security professionals and hackers have long known that end users are the weakest link in organization cyber security (West, 2008). Although much of the responsibility for cyber security rests with employees (Hong, 2012), the average person discriminates between untrustworthy and truthful messages at a level only slightly better than chance (Bond & DePaulo, 2006). Developing savvy computer and mobile device users is essential to cyber security defense. The process begins by teaching end

users the necessary knowledge, skills and attitudes related to cyber security policies. Organizations have figured out how to support an array of training opportunities for in-house cyber security experts to ensure the integrity of internal and client systems, but they must also provide training that prepares end users to circumvent increasing cyber threats (VanDerwerken & Ubell, 2011).

This paper focuses on training end users with little or no professional cyber security training, for they have the greatest need and opportunity for improvement. The paper reviews what we know about effective approaches to cyber security training for end users and offers suggestions about how HR leaders can respond. Comments on broader job and security architecture are provided for perspective, including a list of potential questions that organizations may use to assess the strength of current training approaches. The paper reviews cyber security policies and competencies that serve as the basis for needs analysis, establishing learning goals and training design. Finally, opportunities for HR, I-O and IT subject matter experts (SMEs) to integrate their skills and enhance capabilities of organizations to counteract cyber security threats are discussed.

The Threat: Users Lack Training to Secure Organizations in Cyber Space

Many organizations currently do not offer any role-specific cyber security training. Emphasis is on technology and systems countermeasures, such as restricted sites, acceptable use policies and password rotation to the near exclusion of human countermeasures like needs assessment and deception detection training. When

education and training occur, they are often perfunctory, episodic and inadequate. Effective organizational strategies against cyber threats include both technological and human detection systems (Wright, Chakraborty, Basoglu & Marett, 2009).

IT Personnel: Present Guardians

By and large, technical training for in-house experts, such as systems administrators, cyber security professionals and engineers, is the responsibility of IT departments. Though cyber security is broader than IT, many cyber professionals consider them one and the same. Usually, IT professionals acquire formal education in their area of expertise. As IT is rapidly evolving, incumbents regularly participate in continuing education to remain current. Venues may include certificate programs, in-house and on-the-job education, professional meetings, self-development, seminars, conferences, simulation exercises and boot camps. Training in-house experts is necessary but insufficient for organizationwide cyber security.

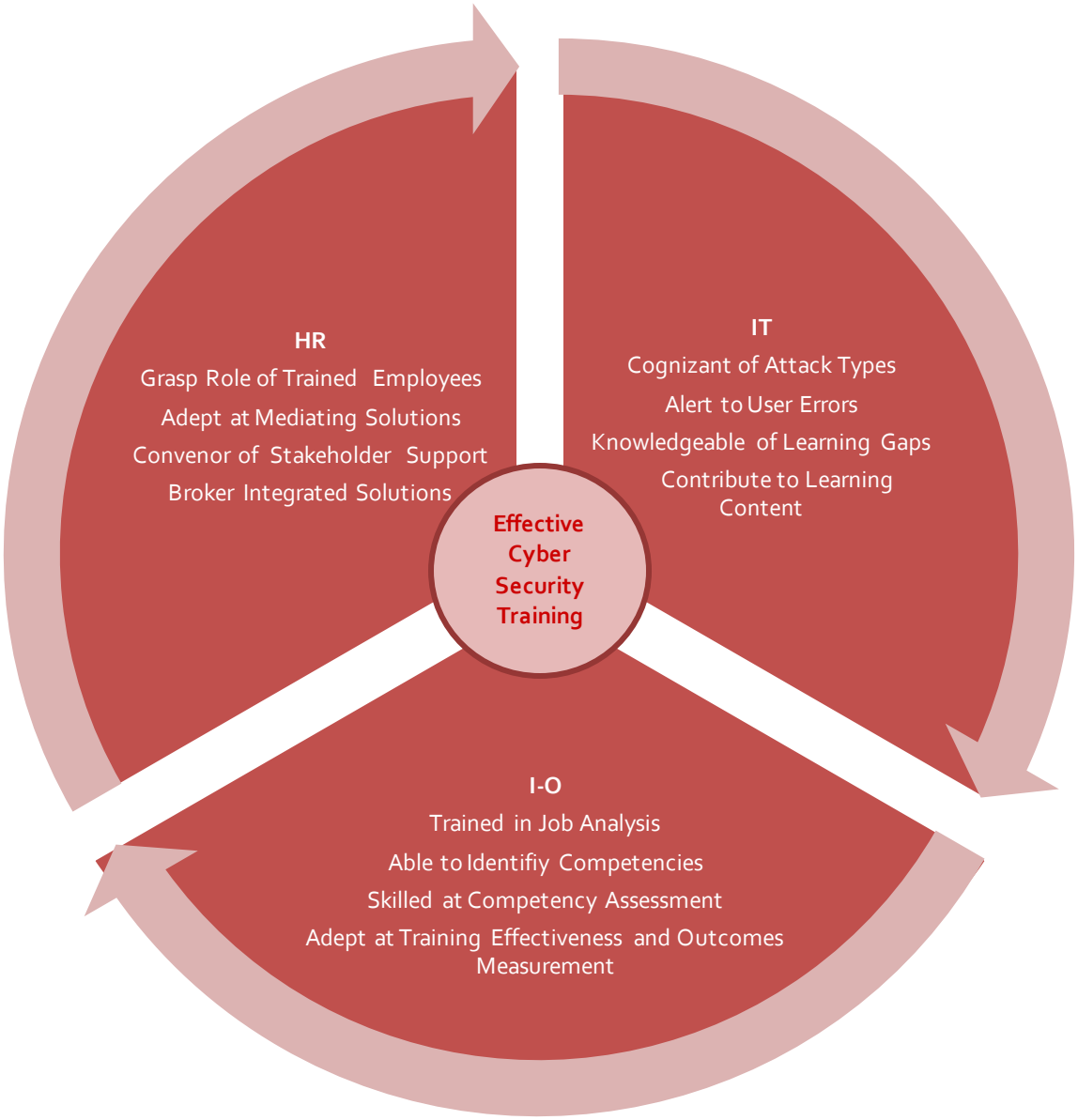
End Users: Potential Defenders

End users must recognize observable phishing cues and lures embedded in computer-mediated messages that commonly appear in websites, e-mails and social networks. As such, they need systematic, coordinated and integrated training to understand trust decisions across these modalities. Moreover, savvy users likely require different training content than naïve users. They need training tailored to their particular learning needs in order to make smart decisions in cyber space.

Current User Training Frequently Is One-Size-Fits-All and Ineffective

Effective cyber security training is difficult to do well. Security awareness training for end users is often too broad and sporadic to cultivate compulsory skills for safe operation on networks. Responsibility for cyber security dwells in IT, or information security (IS), whereas responsibility for training resides in human resources. Typically, IT specialists lack responsibility for and proficiency in training. HR professionals are uniquely positioned to understand the role of trained employees in cyber risk mitigation and to mediate solutions for an organization's cyber security challenges. However, as generalists, they may not have expertise in the science of learning. I-O psychologists are well-versed in the science of learning, though they may lack technical expertise in cyber defense. Each knows part of the solution; none knows the whole solution. Absent careful integration, the result is disjointed and dysfunctional education and training. Figure 1 depicts the competencies possessed by HR, I-O and IT or IS subject matter experts and highlights the importance of integrating discipline-specific knowledge when designing cyber security training solutions. Properly trained, users have potential to augment, defend and join the ranks of those who are custodians of cyber defense.

Figure 1. Interdisciplinary Education and Training Model



Knowledge Required for Effective User Cyber Security Training Design

For optimum effectiveness, SMEs must identify the competencies required for user job success. They must determine the extent to which users exhibit gaps in know-how, and develop gap-closing strategies.

Competencies Users Need

The nature of employee cyber security roles varies. Required competencies may range from basic awareness to business process skills (Wilson, Stine & Bowen, 2011). These may include skills to mitigate technical risks, capacity to develop policies and governance, and specific practices to achieve regulatory compliance. To evaluate and strengthen cyber defense, SMEs must define roles within the job and security architecture. Once defined, it is possible to evaluate training needs and advance cyber security in the broader system (Brummel et al., in press).

Targeted training programs are designed to achieve goals that meet instructional needs. It is counterproductive to launch training without thorough assessment of role-relevant tasks, behaviors and environment (Goldstein & Ford, 2001). Ascertaining workforce capabilities is an essential step in identifying areas that require behavioral and attitudinal change. Training needs analyses involve asking questions that reveal current organizational end user strengths and development needs. This information allows for appropriate learning objectives to be created for the training. One-size-fits-all training is unwise, given the array of user dispositions and skill levels. Armed with knowledge of employee capabilities and vulnerabilities, organizations can design and implement role-based training that equips users with the requisite skills to elude cyber deception. Role-specific training provides the foundation upon which human countermeasures are built.

Determining Best Cyber Security Practices and Training Needs

It is useful to align education and training programs with best practices by surveying policies, practices and future trends of bellwether organizations. Surveys yield evidence-based feedback for SMEs to compare organizational practices with best practices, identify gaps and propose action plans. An environmental scan of methods other organizations use for teaching employees to identify and thwart cyber threats can inform local efforts to integrate practices, policies and venues into role-specific requirements. Surveys serve as a basis for developing learning objectives, training, policies, practices and security architecture.

To build effective surveys, SMEs must build versions that fit their organizations, giving careful consideration to design logic, choice points and relevant security question categories. Does design logic allow questions that differentiate between policy and practice training for IT and non-IT personnel? What choice points are necessary to identify practice trends? Do respondents contemplate time horizons for addressing cyber security policy and practice areas not implemented? Do surveyed organizations differentiate between education and training venues for IT and non-IT personnel? Are timelines anticipated for implementing methods not used? Survey areas may include restricted sites and downloads, acceptable use policy, workforce mobility security, and password management. The Appendix provides an example of survey questions and structure to guide readers seeking evidence-based survey data on best policies and practices. HR managers play an instrumental role in convincing

organizations to gather these data. Acted upon, survey findings empower organizations to build front lines of defense that are more impervious to cyber-attacks.

Competencies Users Possess

Training needs analysis provides information on which to build evidence-based learning. Used to assess employee competencies and learning needs, the essence of the training needs analysis is gap analysis. It assesses gaps between users' existing knowledge, skills and attitudes and those required for on-the-job success. Exploration into psychological, experiential, technological and environmental factors affecting individual dispositions of trust and suspicion is frequently not founded on the ability of end users to perceive cues available to them. Surveys provide evidence for identifying, targeting and designing training that addresses the peculiar learning requirements of incumbents in the job hierarchy, including those of a cyber security nature.

Toward this end, SMEs must **first** examine the job and specific cyber security functions by level for employees in the organization. This step is rooted in job analysis. I-O psychologists can play a crucial role in this phase of the process, due to their education and training related to job analysis. **Second**, I-O psychologists are especially capable of performing analysis where it may not exist and guiding SMEs to a clearer understanding of competencies required to successfully perform essential job functions. **Third**, when performing training needs analysis, it is crucial for those involved to assess whether employees competently perform role-required tasks. When performance gaps appear that are caused by competency deficits, the specialized training of I-O psychologists is invaluable for leading efforts to build gap-closing

training content. **Fourth,** training needs analysis serves as a basis upon which to develop objectives that impart specified knowledge, skills and attitude levels commensurate with task requirements. **Fifth,** SMEs must determine which methods best support objectives and conduct training. This step is advanced by the aforementioned employer survey, because it yields useful information about best practices. **Sixth,** SMEs must evaluate training effectiveness and determine whether it has produced anticipated outcomes, in terms of acquired knowledge, skills, abilities, attitudes and performance. I-O psychologists are proficient in processes used to measure the efficacy of education and training. **Seventh,** data are used to adapt training or adopt nontraining solutions.

Staggs, Beyer, Mol, Fisher, Brummel and Hale (2014) have developed a taxonomy that identifies, classifies and organizes human-perceptible cyber trust cues used to make online trust decisions across web, e-mail and social networking domains. This type of resource is useful for developing content-specific training needs analysis survey questions. The taxonomy delineates various types of cyber deception that end users are likely to encounter and defines the body of knowledge that ought to serve as the foundation for future development of cyber security education and training. It is a lens to examine end user competencies, define training objectives, evaluate training effectiveness and measure organization outcomes with respect to phishing. SMEs must select some means to identify the types of cyber fraud experienced by their organizations and evaluate the extent to which non-IT employees are exposed.

To illustrate, suppose your organization has become concerned about losses arising from the taxonomy category URL obfuscation—genuine-appearing URLs surreptitiously altered to deceive employees. Interdisciplinary SMEs recommend administering a training needs analysis survey to assess the ability of end users to discern deceptively altered URLs and conducting an analysis of results to evaluate strengths and development needs. If results indicate users struggle to distinguish trustworthy URLs from fraudulent ones, users and the organization are vulnerable to typejacking domain name attacks. Cyber crooks commit this type of deception by altering legitimate domain names (e.g., www.paypal.com to www.paypa1.com). In the first instance "paypal" is correctly displayed. In the second instance, the numeral "1" has been substituted for the letter "l," which may lure end users into disclosing personally identifiable or financial information to illegitimate sources.

After administering the training needs analysis survey, conducting an analysis of results and concluding that employees are vulnerable to URL obfuscation, SMEs establish training objectives, design content and propose methods to address this ploy. Training content is taught to those deficient in URL obfuscation detection. Differential training strategies are important, as there is no need to train employees proficiently detecting URL obfuscation. To assess training effectiveness, SMEs can use a parallel test format. Some organizations issue decoy messages with obfuscated URLs to determine whether employees have mastered what they were supposed to learn.

Training Methods that Fill the Gap

Organizations must determine which methods most effectively teach users to recognize cyber threats, operate applications safely and comply with policies. Common methods include mandatory training, instructional e-mail from IT, department training and self-phishing. Self-phishing occurs when IT distributes to employees decoy computer-mediated messages embedded with cues and lures that they are expected to catch. Mock cyber-attack exercises safely simulate deception, expose vulnerabilities, highlight learning needs and provide feedback on training effectiveness.

Measuring Training Effectiveness

The final step is to assess whether the learning process inspired users to apply what they learned. Did they transfer lessons learned to their jobs? Did training produce results (e.g., fewer cyber-attack breaches, fewer cyber-related losses)? What is the return on investment associated with any reduction in obfuscation detection failure? Information derived from targeted training programs provides valuable feedback for improving program content, methods, outcomes and results. Knowledge about the types of cyber deception is optimized when used to create training modules that equip computer users to spot cues embedded in computer-mediated messages. HR practitioners and fellow SMEs aware of this and related research can seize the opportunity to integrate science with practice by applying evidence-based findings to real-world challenges.

A Manageable Challenge with an Interdisciplinary Team

HR practitioners perform roles that allow them to broker solutions and serve as arbiters and conveners of SMEs whose complementary competencies are needed to address complex end user cyber security challenges. It is essential that HR, I-O and IT SMEs coalesce for the purpose of developing comprehensive education and training. Without concerted effort to access the expertise of all three disciplines, cyber defense measures are less effective and organizations are more susceptible to damaging attacks from cyber thieves. To target education and training, interdisciplinary SMEs must collaborate to identify fraudulent message types their organizations have encountered, determine whether end users avoided deception and evaluate existing gaps in know-how. Properly trained, end users develop skills required to confidently and safely navigate cyber space at work and at home.

The Role of HR

HR practitioners are favorably positioned to play a pivotal role in ensuring cyber security competencies of end users. The lack of rigorous role-specific employee training is a flaw in the cyber security strategies of many organizations. Although the SANS Institute, NYU Polytechnic Institute and other notable organizations provide comprehensive training for IT specialists, the lack of effective end user training on savvy practices in the cyber domain remains a significant concern. HR practitioners have an opportunity and responsibility to address this weakness. Their broad gauge responsibility positions them to engender organizational support and convene SMEs whose collective competencies match the complex challenges posed by a need for role-

specific training. VanDerwerken and Ubell (2011) suggest that organizations must systematically train employees and build an army of cyber warriors. Though not all employees will become cyber experts, employers can hold trained users accountable for cyber defense performance apropos of the roles they perform.

The Best Approach: Interdisciplinary

I-O psychologists are comprehensively trained in the scientific processes of job analysis, identifying competencies, learning needs assessments, establishing targeted training objectives, designing effective training programs, and measuring outcomes. The ideal approach is one where HR professionals and IT specialists collaborate with I-O psychologists or develop competencies in these scientific processes themselves to achieve the same end. The latter is often impractical, due to the extensive additional education involved. Competencies possessed by interdisciplinary SMEs comprise those necessary to address role-specific education and training.

Collaboration is also smart when assessing user learning gaps, developing differentiated training program content and identifying the visual cues employees must discern to escape cyber deception. Unified efforts better enable users to detect deceitful messages, avoid harmful effects and share the attributes of fraudulent messages with stakeholders.

A Vision for the Role of HR: Securing the End User

As organizations, systems and technologies have become more complex, professional specialization has resulted. Specialization has produced both advantages and disadvantages. It allows incumbents to develop in-depth expertise in a particular

discipline (e.g., HR, I-O and IT). However, specialization can create silos, myopic perspectives and organization disintegration. It is difficult for one discipline to form a holistic picture of the challenge. This occurs in the field of medicine. That is why primary care providers, or general practice physicians, coordinate medical consultation, diagnosis and patient treatment by providing health care congruent with their core competencies, and access the expertise of other medical specialists. Similarly, HR generalists can improve their effectiveness by providing services commensurate with their core competencies and by partnering with specialists to provide holistic cyber defense solutions.

The role for HR practitioners, then, in securing end users is that of convener, integrator and broker of integrated solutions. Strategically, HR practitioners are positioned to integrate the science of I-O psychology with the practice of human resource management. As conveners, they function in roles that provide opportunities to broker cyber solutions that grow out of the experience and conviction of an interdisciplinary team of SMEs. They can forge whole solutions that access the expertise of relevant disciplines, integrate science with practice and achieve outcomes superior to those derived independently.

Suggestions for Implementing Training Specific to End User Roles and Abilities

To train effectively, it is essential to understand role hierarchy and security architecture. According to Wilson, Stine and Bowen (2011), the targeted training level strives to produce needed security skills and competencies for end users. The education

level merges security skills and competencies of various functional specialties into a common body of knowledge, adds multidisciplinary concepts plus social and technological precepts, and attempts to produce IT security professionals capable of vision and proactive response (Wilson et al., 2011).

IT professionals integrate the tenets of the IT security field in a prospective manner to keep up with technology trends and evolving security implications. At the targeted training level, specific knowledge and skills acquired may become obsolete as technology changes. The exploratory nature of education differentiates it from targeted training. Advances in thought and theory migrate their way into security practices taught in targeted training programs. Educated IT security professionals acquire a comprehensive understanding of the field required to take responsibility for continued learning in an ever-changing environment (Wilson et al., 2011).

At the advanced level of IT security professionalization, such as that of an IT security program manager, employees are expected to engage in addressing inter-organization issues. Examples may include increasing the effectiveness of assurance techniques, developing security policy models and contributing to, developing or managing training programs. To reach advanced level of IT security professionalization, formal education in the field is usually required (Wilson et al., 2011). In targeted training environments, users are taught to use specific skills as part of job performance. In educational contexts, personnel are encouraged to examine and evaluate not only skills and methods of work but also basic operating principles upon which job skills are based. Table 1 presents a summary of the levels and objectives of training and education.

Table 1. Comparative Cyber Security Training Framework

Level	Description
Targeted	Produce non-IT cyber security skills to exact role-specific performance
Education	Cultivate IT security insight and understanding to develop professionals with vision and proactive response capability
Advanced	Equip IT security professionals to address assurance techniques, policy and training

Conclusion

Solutions to cyber security training challenges require an interdisciplinary approach. SMEs must collaborate to optimize employee-focused cyber defense safeguards. To develop targeted role-specific training, they must identify end user knowledge gaps. IT and IS specialists are aware of the cyber fraud types plaguing their organizations and where vulnerabilities exist. A training needs analysis approach facilitates ascertaining strengths, weaknesses, training needs, learning objectives and performance outcomes. HR practitioners are positioned to champion the role of computer-savvy employees in cyber risk mitigation, garner support for end user training, convene SMEs with competencies to match the challenge and broker integrated solutions. I-O psychologists are uniquely qualified to measure whether training is well-designed, role-specific, effective and has achieved desired outcomes. SMEs play an integral role in the solution. Our complex, specialized and sometimes evil world demands that those who develop strategic cyber security solutions are mindful of the age-old precept—a rope of three cords is hard to break.

Take-Home Check List for HR Practitioners

- ☐ Ensure that employee training on cyber security is a strategic organizational priority.
- ☐ Collaborate with IT specialists and I-O psychologists to generate and sustain support.
- ☐ Assemble an interdisciplinary team to develop comprehensive cyber security training.
- ☐ Survey bellwether cyber security practices for integration into education and training.
- ☐ Establish level-specific job and cyber security tasks for employees in the organization.
- ☐ Determine whether employees are currently performing required cyber security tasks.
- ☐ Design training objectives to align knowledge, skills and attitudes with task demands.
- ☐ Choose appropriate venues and methods for learning objectives and conduct training.
- ☐ Assess education and training results to gauge whether organization objectives are met.
- ☐ Adapt education and training initiatives or shift to nontraining solutions when needed.

References

Beyer, R., Mol, M., Haney, M., Staggs, J., Brummel, B., Hale, J. (2014). Organizational Cybersecurity Education and Training: Best Practices and Future Trends

Brummel, B., Hale, J., & Mol, M. (in press). Training cyber security personnel. In S. Zaccaro, R. Dalal, and L. Tetrick, (Eds.), *The Psychosocial Dynamics of Cyber Security*. Taylor & Francis.

Bond, C. F., & DePaulo, B. M. (2006). Accuracy of deception judgments. *Personality and Social Psychology Review, 10,* 214-234.

Goldstein, I. L., & Ford, J. K. (2001). *Training in Organizations*. Belmont, CA: Wadsworth.

Hong, J. (2012). The state of phishing attacks. *Communications of the ACM, 55*(1), 74-81.

Staggs, J., Beyer, R., Mol, M., Fisher, M., Brummel, B., & Hale, J. (2014). A perceptual taxonomy of contextual cues for cyber trust. *Proceeding of the Colloquium for Information System Security Education (CISSE), 2,* 152-169.

VanDerwerken, J., & Ubell, R. (2011). Training on the Cyber Security Frontlines. *T + D, 65*(6), 46-50, 46.

West, R. (2008). The psychology of security. *Communications of the ACM, 51*(4), 34-40. doi: 10.1145/1330311.1330320

Wilson, M., Stine, K., & Bowen, P. (2011). National Institute of Standards and Technology (NIST) Special Publication 800–16: Information technology security training requirements: A role-and performance-based model (Draft): Nov.

Wright, R., Chakraborty, S., Basoglu, A., & Marett, K. (2009). Where did they go right? Understanding the deception in phishing communications. *Group Decision and Negotiation, 19,* 391-416. doi: 10.1007/s10726-009-9167-9.

Appendix

Organizational Cybersecurity Education and Training: Best Practices and Future Trends
Example Items (full survey available on request from the first author)

Q. On which of the following policy or practice areas does your company **educate and train end users**? For those areas that you do not currently provide education or training, please indicate the expected time horizon (if any) for implementation.

	Time Horizon for Implementation							
	Currently Imple-mented	< Six Months	Six Months	One Year	Two Years	Five Years	Never	Don't Know
Restricted sites and download	☐	☐	☐	☐	☐	☐	☐	☐
Acceptable-use policy	☐	☐	☐	☐	☐	☐	☐	☐
Workforce mobility security (e.g. secure Internet connection, VPN, safety, etiquette)	☐	☐	☐	☐	☐	☐	☐	☐
Cybersecurity competency testing	☐	☐	☐	☐	☐	☐	☐	☐
Deception detection training for e-mails, web, social networking, downloads (e.g., visual spoofing, phishing cues, etc.)	☐	☐	☐	☐	☐	☐	☐	☐
Password management (e.g., change frequency, construction and protection standards)	☐	☐	☐	☐	☐	☐	☐	☐
Employee departure data security procedure	☐	☐	☐	☐	☐	☐	☐	☐

Q. Which of the following methods does your company use to **educate and train end users** about **companywide policies or practices**? For the matrix below: S = seminars and conferences, Boot Camps = boot camps and other intensive trainings, CSC = cyber security specific communications (e.g., lunch and learns, newsletters, memoranda, face-to-face, intranets), SE = simulation exercises, CIT = critical incident training. Select all that apply.

	Time Horizon for Implementation					
	S	Boot Camps	CSC	SE	CIT	NA
Restricted sites and download	☐	☐	☐	☐	☐	☐
Acceptable-use policy	☐	☐	☐	☐	☐	☐
Workforce mobility security (e.g. secure Internet connection, VPN, safety, etiquette)	☐	☐	☐	☐	☐	☐
Cybersecurity competency testing	☐	☐	☐	☐	☐	☐
Deception detection training for e-mails, web, social networking, downloads (e.g., visual spoofing, phishing cues, etc.)	☐	☐	☐	☐	☐	☐
Password management (e.g., change frequency, construction and protection standards)	☐	☐	☐	☐	☐	☐
Employee departure data security procedure	☐	☐	☐	☐	☐	☐