Online Journal of Applied Knowledge Management
A Publication of the International Institute for Applied Knowledge Management

Volume 5, Issue 2, 2017

Cybersecurity skills: Foundational theory and the cornerstone of advanced persistent threats (APTs) mitigation

Melissa Carlton, Nova Southeastern University, melissa.carlton.phd@gmail.com

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

Abstract

Cyber threats have been growing with social engineering and business e-mail compromise reported as the two most rising penetration vectors. Advanced Persistent Threats (APTs) are penetration techniques that combine several approaches to gain access to organizational networks. Organizations need a team of skilled individuals to mitigate or prevent the complexity and seriousness of cyber threats such as APTs. A skill is defined as the combination of ability, knowledge, and experience to do something well. Therefore, cybersecurity skills correspond to individual's ability, knowledge, and experience surrounding the hardware and software required to identify, protect, detect, respond, and recover against damage, unauthorized use, modification, and/or exploitation of cyber infrastructure. Moreover, a strong security posture cannot exist without individuals that possess high level of cybersecurity skills as cyber-attackers prejudice against all nationalities. Therefore, the importance to find individuals that use their cybersecurity skills for good is paramount. This paper presents an-in-depth discussion on the theoretical rationale for cybersecurity skills as the cornerstone of APTs and other cyber threat mitigation.

Keywords: Cybersecurity skills, cybersecurity knowledge, cybersecurity experience, cybersecurity ability, advanced persistent threats mitigation, social engineering mitigation

Introduction

Cyber threats have been continuously growing with social engineering and business e-mail compromise reported to be the two most growing penetration vectors to most organizations (Federal Bureau of Investigation, 2017). While cyber threats have been growing, Information Technology (IT) security functions at 70% of organizations surveyed by Ponemon Institute (2014) were found understaffed. Moreover, APTs are penetration techniques used by cybercriminals that mix several approaches, including social engineering and business e-mail compromise, to gain access to organizational networks, harvest critical proprietary data, and avoid detection for a longer duration of time (Symantec, 2017). The complex and serious cyber threats such as APTs, both internal and external, faced by an organization cannot be mitigated without a strong security posture that includes a team of skilled professionals (Ponemon Institute, 2014). It is difficult to find individuals that desire to use their cybersecurity skills for good and not evil given that the rewards from cyber attacks are significant (Hueca, Clarke, & Levy, 2016;

Rastello & Smialek, 2013). Furnell and Moore (2014) found that 57% of digital leaders surveyed indicated a need for the existing workforce to have enhanced IT skills. According to the U.S. Department of Labor (2014), Information System (IS) security positions are predicted to grow 37% from 2012 to 2022. Waiting until high school to feed the excitement about science, technology, engineering, and math (STEM) appears to be too late. According to the commissioner for the Air Force Association's CyberPatriot contest, feeding the technical workforce starts with getting teenagers, even pre-teens, excited about STEM in middle-school (Rastello & Smialek, 2013). Unfortunately, for majority of these young adults, ages 18 to 26, it is too late as cybersecurity skills were not taught in their middle-school classrooms (Raytheon – National Cyber Security Alliance (NCSA), 2015). To close the gap in cybersecurity skills establishment and development, it must first be defined, then analyzed closely, which is the focus of this paper.

Skills defined

A skill is defined as the combination of abilities, knowledge, and experience that enables an individual to complete a task well (Boyatzis & Kolb, 1991; Carlton, Levy, Ramim, & Terrell, 2015; Levy, 2005). Acquiring a skill generally adopts three incremental stages and is a learning process (Anderson, 1982; Gravill, Compeau, & Marcolin, 2006). The initial acquisition of a skill known as declarative knowledge (Stage 1) that begins the learning process. According to Anderson (1982) as well as Fitts (1964), instructions and information about a skill are given to the individual at this stage. The knowledge established and internalized in Stage 1 becomes the foundation for later learning stages (Gravill et al., 2006; Nonaka, 2008). The learner is allowed to practice declarative knowledge and covert it to procedural knowledge during the second stage (Stage 2) of acquiring a skill (Fitts, 1964; Neves & Anderson, 1981). As individuals begin to connect the actions needed to accomplish a task, knowledge becomes better arranged in a systematic way, which enables value to them and the organizations they work for (Gravill et al., 2006; Russ, Jones, & Fineman, 2006). Automaticity comes next at the third stage of skill acquisition (Fitts, 1964; Marcolin, Compeau, Munro, & Huff, 2000). The increase in experience level allows an individual to progress past the initial acquisition stage into a well-organized and autonomous Stage 3 (Anderson, 1982; Gravill et al., 2006).

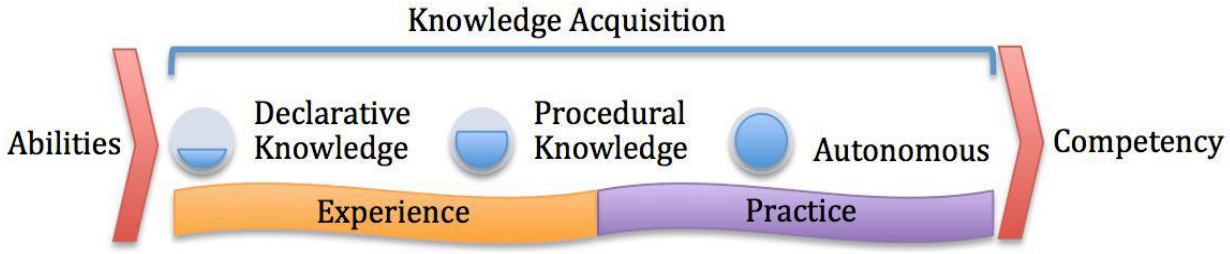

Figure 1. The Stages of Skill Development and Competency Attainment

It is known from research that an individual's technology usage experience positively influences and helps establish the needed know-how of the skill (Gravill et al., 2006). The phases of knowledge acquisition allow individuals to develop the ability to generalize procedures to new tasks and increase performance by moving into a more fluid and efficient progression towards competency (See Figure 1) (Marcolin et al., 2000). Competencies are acquired over time as the breadth and depth of an individual's knowledge increases through experience related to that skill or set of skills (Eschenbrenner & Nah, 2014; Benilian, 2015).

Cybersecurity skills

According to the National Initiative for Cybersecurity Careers and Studies (NICCS), cybersecurity is "the activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation" (2014, Cybersecurity section, para. 1). The restoration of digital information and communication is also included in cybersecurity (Axelrod, 2006). An environment for a potential information security breach exists with an individual without the skills to use a cybersecurity tool or an unusable cybersecurity tool (Nurse, Creese, Goldsmith, & Lamberts, 2011). Furthermore, an individual not aware of all the cybersecurity tool features poses yet another opportunity for an information security breach. Moreover, if an individual is not fully knowledgeable of a cybersecurity tool's functionality, they may have a false sense of confidence that they are skilled in using the tool to mitigate cyber-attacks (Gibbs, Moore, Steel, & McKinnon, 2017). Therefore, the code of practice for organizations to apply information security controls was established by the International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) (2013). To ensure the appropriate information security skills and qualifications are maintained, regular offerings of employee training is among these information security controls (ISO/IEC 27002, 2013; Spruit & Röling, 2014). Moreover, the cybersecurity system development processes encourages cybersecurity tool usage including the human and social aspects (Nurse et al., 2011).

Despite the advances in IT when it comes to corporate IS, individuals, even with the best intentions, falling victim to social engineering attacks appear to prevail in eluding such IT defenses (Mitnick & Simon, 2002; Hernandez, Levy, & Ramim, 2016). IT users' errors, due to poor cybersecurity skills, represent the weakest link in an organization's IS security (Carlton & Levy, 2015). Knowledge protects valuable information from increasingly elaborate cyber threats, such as APTs (Enterprise Risk Management (ERM), 2014). Therefore, cybersecurity skills correspond to an individual's technical ability, knowledge, and experience surrounding the hardware and software required to implement IS security for mitigating a cyber-attack (Carlton et al., 2015; Choi, Levy, & Hovav, 2013). The necessity for individuals to exhibit cybersecurity skills is not restricted to a single vocation or industry (Burley et al., 2014). According to the Anti-Phishing Working Group (APWG) (2017), identified cyber threats targeted retail, financial, payment services, and Internet Service Providers (ISPs). Furthermore, the top cybersecurity threats and the respective skills identified by subject matter experts were platform independent and grouped into three distinct categories: work information systems, malware, and personally

identifiable information (Carlton & Levy, 2015). "Knowledge, skills, and abilities are needed for more than cybersecurity work" (Carlton & Levy, 2015, p. 3). Likewise, an individual knowledgeable about IT does not instinctively generate a cybersecurity savvy individual (Choi et al., 2013; Gibbs et al., 2017). Thus, it appears a limited cybersecurity skilled individual may propagate opportunities for organizational IS vulnerabilities and threats (Carlton, 2016; Thomson & von Solms, 2005).

Competence

Prior research such as Bronsburg (2011) as well as Morcke, Dornan, and Eika (2013) spoke to the importance of demonstrated high-level skills in the medical and health profession academic programs. Moreover, the utilization of scenario-based, hands-on assessments to measure pilots' skills as mandated by the Federal Aviation Administration (FAA) may be found in aviation academic curriculum (Thomas & Lee, 2015). Competencies, skills, knowledge, and abilities are interconnected and important to include in the classroom so students have the experience necessary for future employment (Havelka & Merhout, 2009; Rubin & Dierdorff, 2009). College and university course offerings are pertinent to a student's competency level (Rubin & Dierdorff, 2009). Furthermore, coursework disseminates knowledge and enables the development of tacit knowledge (Havelka & Merhout, 2009; Russ et al., 2006). Competency based learning and computer simulations in an online learning environment enhanced management skills significantly (Levy & Ramim, 2015). Moreover, various teaching methodologies provide students with academic experience to develop and strengthen specific skills for supporting their occupations (Levy & Ramim, 2015).

Eschenbrenner and Nah (2014) found competency was developed through the maturing of an individual's knowledge as a result of improved skills. Additionally, Toth and Klein (2014) noted that competencies were developed as individuals gathered knowledge and honed skills. When course offerings and required corporate competencies are misaligned, and individual's exposure to important knowledge to do a task well is reduced (Rubin & Dierdorff, 2009). The influence of an individual's competency level of a particular skill may even determine an individual's professional satisfaction level (Havelka & Merhout, 2009; Levy & Ramim, 2015). An individual's competence is crucial to an organization that depends on its employees to have the right skills (i.e., abilities, knowledge, & experiences) to complete tasks successfully (Downey & Smith, 2011). In order to accomplish something successfully and responsibly, competencies are needed (Adomßent & Hoffman, 2013; Beaudoin, Kurtz, & Eden, 2009). Competence with IT has an effect on workplace productivity and empowers individuals (Marcolin et al., 2000). As seen in Figure 2, abilities, knowledge, and experience forms and increases skill level, when practiced over time develops competency (Carlton & Levy, 2015; Levy & Ramim, 2015). Tenison, Fincham, and Anderson (2016) found individuals took on average five to six practice attempts before having the ability to recall the correct answer to a problem. Thus, the need for cybersecurity skilled individuals and cybersecurity mitigation tools is paramount as one successful cyber-attack attempt may result in substantial financial and information losses (Carlton, 2016).

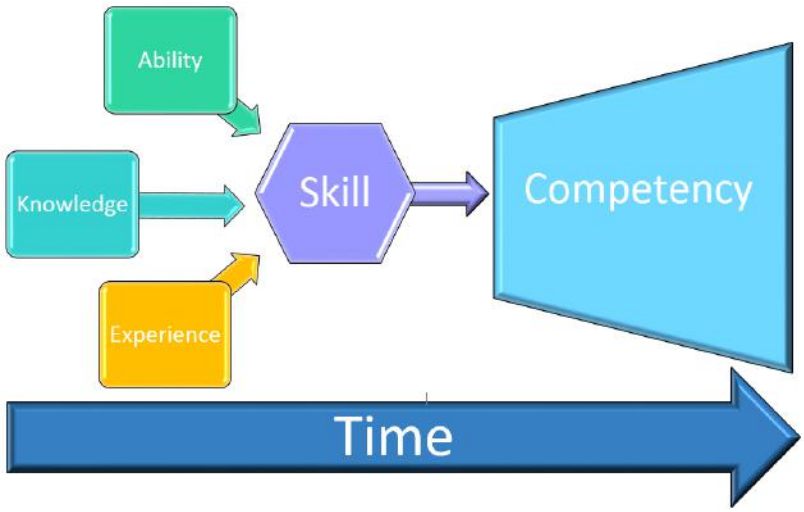

Figure 2. Skill Over Time Develops Competency

Cybersecurity risk and mitigation tools

Protecting or defending against cyber-attacks, involves both technical and human ability (Committee on National Security Systems (CNSS), 2010). Risk is defined as a "measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would rise if the circumstance or event occurs; and (ii) the likelihood of occurrence" (National Institute of Standards and Technology (NIST), 2006). Therefore, any disruption of operations and financial loss caused by a malevolent cyber event describes cybersecurity risk (Mukhopadhyay, Chatterjee, Saha, Mahanti, & Sadhukhan, 2013; NIST, 2014). An organization or individual performing risk mitigation is "prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process" (CNSS, 2010, p. 62). Risk mitigation is essential to guard IS systems as individuals making unintentional errors compromise IS security (Maxion & Reeder, 2005). Moreover, common hardware attacks involve hardware Trojans, illegal clones, and side channel attacks, i.e., snooping hardware signals (Jang-Jaccard & Nepal, 2014). Whereas, common software attacks included software programming bugs, such as memory management, user input validation, race conditions, and user access privileges. As technologies emerge (e.g., self-driving cars, embedded systems & sensors, etc.) and proliferation of Internet-of-Things (IoT) devices, the need to guard and defend against cyber threats and vulnerabilities increases (Jang-Jaccard & Nepal, 2014; Ransbotham, Mitra, & Ramsey, 2012). In 2013, former United States President Barak Obama issued Executive Order No. 13,636 in response to the cybersecurity threats "placing the Nation's security, economy, and public safety and health at risk" (NIST, 2014, p.1). Executive order No. 13,636 addressed the need for improving the critical infrastructure systems and established that "the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber-environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties" (p. 11739).

Furthermore, the Executive Order 13,636 (2013) summons for the making of the 'Cybersecurity Framework' that includes "a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks" (p. 11741).

Through a collaboration of government, academia, and private sector partners, NIST (2014) created a common language, cost effective, non-regulatory 'Cybersecurity Framework' that addresses and provides a voluntary roadmap to manage cybersecurity risk. According to NIST (2014), the 'Framework' is scalable and evolving as technology advances and business requires. But, revisions to the 'Framework' are expected once every other year (NIST, 2017). Based on existing standards, guidelines, and practices, incorporating the 'Framework' into an organization's operations is voluntary as it complements an organization's risk mitigation and cybersecurity program (NIST, 2014; 2017). Consisting of five functions (Identify, Protect, Detect, Respond, & Recover), the 'Framework Core' assists management of cybersecurity activities manage cybersecurity risk at their highest level as seen in Figure 3 (NIST, 2014; 2017).

Figure 3. The NIST Cybersecurity Framework 1.1 (2017)

Discussion and future work

The demand for employees with skills to protect information systems and the information contained with those systems will continue to rise as cyber-attacks increase (U.S. Department of Labor, 2014). The nexus of this paper is that cybersecurity skills are the cornerstone of APTs and other cyber threat mitigation. Vulnerabilities of individuals, organizations, or governments conducting transactions online are exploited by hackers and cyber criminals with skills (Cox, 2015). Cyber-attacks are not biased by nationality. For example, the Prime Minister of the United Kingdom, David Cameron, addressed the need for skilled individuals to protect his nation (United Kingdom, 2015). Similarly, the Prime Minister of Israel, Benjamin Netanyahu, indicates

that highly competent individuals with the proper cybersecurity skills are "an essential condition for national security and economic growth in the 21st century" (Globes, 2016). Closing the gap in what skills individuals need and the skills they demonstrate will assist in their learning of competencies needed for successful work performances (Levy & Ramim, 2017). Thus, in the United States, the Joint Task Force (JTF) on Cybersecurity Education (CSEC2017) is working to "develop comprehensive curricular guidance in cybersecurity education" (2017, p. 7). The CSEC2017 JTF efforts will then be disseminated to national and international programs that offer a cybersecurity undergraduate degree, with a recommended set of required hours each program should maintain on the various knowledge areas and skill development topics. These recommendations will then serve as the basis for the development of students' cybersecurity skills during regular courses in efforts to graduate them with the appropriate competences. Moreover, CSEC2017 will link together these knowledge areas and skill development topics with specific computing programs (i.e. Disciplinary Lenses: Computer Science, Computer Engineering, Software Engineering, Information Technology, Information Systems) and include mapping to specific courses and labs.

There are many areas for future work in cybersecurity skills given that, as argued above, it serves as the theoretical foundation and cornerstone for cyber threat mitigations. The first recommendation includes investigating the effects, if any, between the education level as well as other demographic variables and demonstrated cybersecurity skills level of an individual. The second recommendation is to develop tools that will assist individuals in strengthening their cybersecurity skills without negative effects to existing systems. Last, the Cybersecurity Skills Index (CSI) benchmarking and mitigation tools developed by prior researchers (i.e., Carlton et al., 2015) may help organizations assess cybersecurity skills of their employees and map them to appropriate categories in order to recommend those at the lower margins to obtain additional knowledge and experiences to elevate their skill levels to help protect against cyber threats. Moreover, it appears that additional research is needed to uncover the situation in less developed countries, given that finding skilled, knowledgeable employees appear to be more difficult. Furthermore, additional research is needed to better understand how to create appropriate conditions for the excitement about cybersecurity in the context of STEM programs for middle and high schoolers.

Acknowledgement

We would like to thank the anonymous reviews for their constructive comments and suggestions to enhance the quality of this paper. We also would like to thank Professors Meir Russ and Nitza Geri for their valuable comments in improving this paper. Prior work that lead to this manuscript was funded by the Nova Southeastern University (NSU) President's Faculty Research and Development Grant (PFRDG).

References

Adomßent, M., & Hoffman, T. (2013). *The concept of competencies in the context of Education for Sustainable Development (ESD)*. Retrieved from http://esd-expert.net/assets/130314-Concept-Paper-ESD-Competencies.pdf

Anderson, J. R. (1982). Acquisition of cognitive skill. *Psychological Review, 89*(4), 369-406.

Anti-Phishing Working Group (APWG). (2017). *Phishing activity trends report (4th quarter 2016).* Retrieved from http://docs.apwg.org/reports/apwg_trends_report_q4_2016.pdf

Axelrod, C. W. (2006). Cybersecurity and the critical infrastructure: Looking beyond the perimeter. *Information Systems Control Journal, 6*(3). Retrieved from http://www.isaca.org/Journal/Past-Issues/2006/Volume-3/Pages/Cybersecurity-and-the-Critical-Infrastructure-Looking-Beyond-the-Perimeter1.aspx

Beaudoin, M. F., Kurtz, G., & Eden, S. (2009). Experiences and opinions of e-learners: What works, what are the challenges, and what competencies ensure successful online learning. *Interdisciplinary Journal of E-Learning & Learning Objects, 5*, 275-289.

Benilian, A. (2015). IT feature use over time and its impact on individual task performance. *Journal of the Association for Information Systems, 16*(3), 144-173.

Boyatzis, R. E., & Kolb, D. A. (1991). Assessing individuality in learning: The learning skills profile. *Educational Psychology, 11*(3/4), 279-295.

Bronsburg, S. E. (2011). *The impact of an osteopathic medical program on information technology skills of physicians entering the workforce* (Doctoral dissertation). Retrieved from ProQuest Dissertations and Theses. (UMI No. 3465615)

Burley, D. L., Eisenberg, J., & Goodman, S. E. (2014). Privacy and security: Would cybersecurity professionalization help address the cybersecurity crisis? *Communications of the ACM, 57*(2), 24-27.

Carlton, M. (2016). *Development of a cybersecurity skills index: A scenarios-based, hands-on measure of non-IT professionals' cybersecurity skills* (Doctoral dissertation). Retrieved from ProQuest Dissertations and Theses Global. (UMI No. 10240271)

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

Carlton, M., Levy, Y., Ramim, M. M., & Terrell, S. R. (2015). Development of the MyCyberSkills™ iPad app: A scenarios-based, hands-on measure of non-IT professionals' cybersecurity skills. *Proceedings of the Pre-International Conference of Information Systems (ICIS) SIGSEC - Workshop on Information Security and Privacy (WISP) 2015*, Ft. Worth, Texas.

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 (ICIS) SIGSEC – Workshop on Information Security and Privacy (WISP) 2013 (Paper 29)*, Milan, Italy. Retrieved from http://aisel.aisnet.org/wisp2012/29

Committee on National Security Systems (CNSS). (2010, April 26). *National information assurance (IA) glossary* (Instruction No. 4009). Retrieved from http://www.ncix.gov/publications/policy/docs/CNSSI_4009.pdf

Cox, C. (2015). Cyber capabilities and intent of terrorist forces. *Information Security Journal: A Global Perspective, 24*(1-3), 31-38.

Downey, J. P., & Smith, L. A. (2011). The role of computer attitudes in enhancing computer competence in training. *Journal of Organizational and End User Computing, 23*(3), 81-100.Enterprise Risk Management (ERM), 2014

Eschenbrenner, B., & Nah, F. F.-H. (2014). Information systems user competency: A conceptual foundation. *Communications of the Association for Information systems, 34*, 1363-1378.

Exec. Order No. 13,636, 78 Fed. Reg. 11739 (2013).

Federal Bureau of Investigation (FBI) (2017). Internet crime complaint center. Retrieved from https://www.ic3.gov/

Fitts, P. M. (1964). Perceptual-motor skill learning. In A. W. Melton (Ed.), *Categories of human learning* (pp. 243-292). New York: Academic Press.

Furnell, S., & Moore, L. (2014). Security literacy: The missing link in today's online society? *Computer Fraud & Security, 2014*(5), 12-18.

Gibbs, S., Moore, K., Steel, G., & McKinnon, A. (2017). The Dunning-Kruger effect in a workplace computing setting. *Computers in Human Behavior*. Advance online publication. doi: 10.1016/j.chb.2016.12.084

Globes. (2016). Israel is a global cyber security power. http://www.globes.co.il/en/article-israel-is-a-global-cyber-security-power-1001114556

Gravill, J. I., Compeau, D. R., & Marcolin, B. I. (2006). Experience effects on the accuracy of self-assessed user competence. *Information & Management, 43*(3), 378-394.

Hernandez, W., Levy, Y., & Ramim, M. (2016). An empirical assessment of employee cyberslacking in the public sector: The social engineering threat. *Online Journal of Applied Knowledge Management, 4*(2), 93-109. Retrieved from http://www.iiakm.org/ojakm/articles/2016/volume4_2/OJAKM_Volume4_2pp93-109.pdf

Hueca, A. L., Clarke, K., & Levy, Y. (2016). Exploring the motivation behind cybersecurity insider threat and proposed research agenda. Proceeding of the Knowledge Management (KM) 2016 Conference, University of Lisbon - ISEG, Lisbon, Portugal, pp. 2-15. Retrieved from http://www.iiakm.org/conference/proceedings/KM_2016_RefereedProceedingsPapers.pdf

Havelka, D., & Merhout, J. W. (2009). Toward a theory of information technology professional competence. *The Journal of Computer Information Systems, 50*(2), 106-116.

International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC). (2013). *ISO/IEC 27002: Information technology – security techniques – code of practice for information security controls*.

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

Joint Task Force on Cybersecurity Education (CSEC2017) (2017). *Cybersecurity curricula 2017* (version 0.5). Retrieved from https://www.csec2017.org/csec2017-v-0-5

Levy, Y. (2005). A case study of management skills comparison in online and on-campus MBA programs. *International Journal of Information and Communications Technology Education, 1*(3), 1-20. doi:10.4018/jicte.2005070101

Levy, Y., & Ramim, M. M. (2015). An assessment of competency-based simulations on e-learners' management skills enhancements. *Interdisciplinary Journal of e-Skills and Lifelong Learning, 11*, 179-190.

Levy, Y., & Ramim, M. M. (2017). The e-learning skills gap study: Initial results of skills desired for persistence and success in online engineering and computing courses. *Proceeding of the Chais 2017 Conference on Innovative and Learning Technologies Research*, The Open University of Israel, Raanana, Israel, pp. 57E-68E. Retrieved from http://www.openu.ac.il/innovation/chais2017/a1_2.pdf

Marcolin, B. L., Compeau, D. R., Munro, M. C., & Huff, S. L. (2000). Assessing user competence: Conceptualization and measurement. *Information Systems Research, 11*(1), 37-60.

Maxion, R. A., & Reeder, R. W. (2005). Improving user-interface dependability through mitigation of human error. *International Journal of Human-Computer Studies, 63*(1-2), 25-50.

Mitnick, K. D., & Simon, W. L. (2002). *The art of deception: Controlling the human element of security.* Indianapolis, IN: Wiley Publishing, Inc.

Morcke, A. M., Dornan, T., & Eika, B. (2013). Outcome (competency) based education: An exploration of its origins, theoretical basis, and empirical evidence. *Advances in Health Sciences Education, 18*(4), 851-863.

Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A., & Sadhukhan, S. K. (2013.). Cyber-risk decision models: To insure IT or not? *Decision Support Systems, 56*(December), 11-26.

National Initiative for Cybersecurity Careers and Studies (NICCS). (2014). *Cyber Glossary*. Retrieved from http://niccs.us-cert.gov/glossary#cybersecurity

National Institute of Standards and Technology (NIST). (2014, February 12). *Framework for improving critical infrastructure cybersecurity* (version 1.0). Retrieved from http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

National Institute of Standards and Technology (NIST). (2017, January 10). *Framework for improving critical infrastructure cybersecurity* (version 1.0). Retrieved from https://www.nist.gov/sites/default/files/documents/2017/01/30/draft-cybersecurity-framework-v1.1.pdf

National Institute of Standards and Technology (NIST), Computer Security Division. (2006, March). *Federal information processing standards publication: Minimum security requirements for Federal information and information systems* (FIPS PUB 200). Retrieved from http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf

Neves, D. M., & Anderson, J. R. (1981). Knowledge compilation: Mechanisms for the automatization of cognitive skills. In J. R. Anderson (Ed.), *Cognitive skills and their acquisition* (pp. 57-84). Hillsdale, NJ: Lawrence Erlbaum Associates, Inc.

Nonaka, I. (2008). *The knowledge-creating company*. Cambridge, MA: Harvard Business Review.

Nurse, J. R., Creese, S., Goldsmith, M., & Lamberts, K. (2011, September). Guidelines for usable cybersecurity: Past and present. In *Cyberspace Safety and Security (CSS), 2011 Third International Workshop on* (pp. 21-26). IEEE.

Ponemon Institute. (2014b). *Understaffed and at risk: Today's IT security department*. Retrieved from HP Enterprise Security website: http://www.hp.com/hpinfo/newsroom/press_kits/2014/RSAConference2014/Ponemon_IT_Security_Jobs_Report.pdf

Ransbotham, S., Mitra, S., & Ramsey, J. (2012). Are markets for vulnerabilities effective? *MIS Quarterly*, *36*(1), 43-64.

Rastello, S., & Smialek, J. (2013, May 16). Cybersecurity starts in high school with tomorrow's hires. *Bloomberg*

Raytheon – National Cyber Security Alliance (NCSA). (2015). *Securing our future: Closing the cybersecurity talent gap.* Retrieved from http://www.raytheoncyber.com/rtnwcm/groups/cyber/documents/content/rtn_278208.pdf

Rubin, R. S., & Dierdorff, E. C. (2009). How relevant is the MBA? Assessing the alignment of required curricula and required managerial competencies. *Academy of Management Learning & Education*, *8*(2), 208-224.

Russ, M., Jones, J. K., & Fineman, R. (2006). Knowledge-based strategies: a foundation of a typology. *International Journal of Information Technology and Management*, *4*(2), 138-165. doi: 10.1504/IJITM.2005.006764

Spruit, M., & Röling, M. (2014). ISFAM: The information security focus area maturity model. *Proceedings of the European Conference on Information Systems (ECIS) 2014*, Tel Aviv, Israel.

Symantec, Inc. (2017). Advanced persistent threats. Retrieved from https://www.symantec.com/

Tenison, C., Fincham, J. M., & Anderson, J. R. (2016). Phases of learning: How skill acquisition impacts cognitive processing. *Cognitive Psychology, 87*(June 2016), 1-28.

Thomas, R., & Lee, C. C. (2015). Development of training scenarios in the flight training device for flight courses at Embry Riddle Aeronautical University. *Journal of Aviation/Aerospace Education & Research, 24*(3), 65-82.

Thomson, K.-L., & von Solms, R. (2005). Information security obedience: A definition. *Computers & Security, 24*(1), 69-75.

Toth, P., & Klein, P. (2014). *A role-based model for federal information technology / cyber security training* (NIST special publication 800-16 revision 1, 3rd draft). U.S. Department of Labor, 2014

United Kingdom. (2015, November). *National security strategy and strategic defence and security review 2015* (Cm 9161). Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.pdf

Authors' Biographies

Dr. Melissa Carlton completed her doctoral studies in Information Systems and Cybersecurity at the College of Engineering and Computing (CEC) at Nova Southeastern University (NSU). She has presented and published in top-tier peer reviewed publications. Her service to the academic community includes ad hoc reviewer/editor, student mentor, as well as co-coordinator and presenter of cybersecurity skills to 200 Miami-Dade high school students as part of Cybersecurity Awareness Day at NSU. She is a member of Levy CyLab, Association for Computing Machinery (ACM), Association for Information Systems (AIS), Institute of Electrical and Electronics Engineers (IEEE), and Upsilon Pi Epsilon honor society.

Dr. Yair Levy 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 e-Learning Security Research, 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 1,400 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 member on of the 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://cec.nova.edu/~levyy/