International Journal of Applied Technology & Leadership
ISSN 2720-5215
Volume 2, Issue 1, January 2023
ijatl@org

Identifying and Engaging Adjoining Career Fields to Increase Cybersecurity Training Efficacy

Ervin Henry Frenzel

Capitol Technology University (USA)

Ian McAndrews, PhD

Capitol Technology University (USA)

Abstract

This paper provides a recommendation guide for connecting existing career fields to various cybersecurity countermeasures to correct an oversight that has long haunted the people, processes, and technology model. The belief cybersecurity only deals with securing technology prevents incorporation of needed skill sets to counter the lack of people skills associated with technology and technologists. Incorporation of people skill experts can greatly enhance the effectiveness of techniques to counter attacks against the people security countermeasure. Analysis of ACM, IEEE, and other existing cybersecurity documentation indicate a need increase training in the people and processes countermeasures to effectively train cybersecurity technicians. ACM and IEEE technology specialists recognize a lack of non-technical skills within the technical fields, technologists need to embrace non-technical specialists who can broaden the base knowledge within cybersecurity. The researched documentation further indicated a potential to cross specialists in the people and processes countermeasures into the cybersecurity career field. Cybersecurity is only effective is all three countermeasures; people, processes, and technology are addressed within an organization. Training technology has long been used as effective cybersecurity training; in truth it is only addressing technology security. To maximize cybersecurity, specialists in the people and processes countermeasures must be brought in to aid training in all of the countermeasures.

Keywords: cybersecurity skills training, non-technical cybersecurity skills training, security countermeasures skills development

1. Introduction

Cybersecurity takes on the overarching perspective of the technology that develops it, whether it is Computer Science, Computer Engineering, Software Engineering, Information Systems Management, Information Technology, or the emerging Data Science field [3][4]. The underlying perspective carried by the individual into their future in the cybersecurity field shapes the lens that the individual will use for the remainder of their life, experiences and education continuously shape an individual's vantage point throughout their life [14][15][3][4]. The weakest skill set for technicians coming from technical fields into the cybersecurity workforce is often soft skills [5][20].

The computer curriculum 2020 Task Force and the Cybersecurity 2017 Task Force recognize that other career fields will have substantially better soft skills than technicians trained in traditional technology fields [20][3][4]. Multi-dimensional cybersecurity professionals must be able to address people, processes, and technologies within the workspace [3][4][17][13][5] [11][12][16]. An infrastructure or information technology cybersecurity technician is either a red *team attacker* or a blue *team defender*. In this paper, no further emphasis or breakdown will occur based upon white or black hats, those with or without work authorization within the organization.

For this paper, technical skills require obtaining identified technical or non-technical skills which develop through either formal or informal studies or experiences in constituent security studies in Computer Science, Computer Engineering, Software Engineering, Information Systems Management, Information Technology, or the emerging Data Science field as defined by IEEE and ACM, the International Standards Organization recognized governing technology bodies [3][4][5]. Non-technical skills are developed through traditional and non-traditional studies of people and their behaviors or processes, this covers many different fields of study including any field dealing with the interaction of individuals, organizations, or states and technology [17][3][4][13][5][11]. The key variation is that technical competence can be in *soft* skills just as much as in a *technical* skill set [20]. Technical competence is in the eye of the beholder; a psychiatrist is more technically competent in mental health diagnostics than in computer diagnostics, while an IT technician is more technically competent in computer diagnostics than in mental health diagnosis. This comparison between different types of STS technician is essential to begin to understand a specialization within the holistic cybersecurity STS includes more than what is encompassed within the software and hardware of a computer.

The distinction between cybersecurity technicians and personnel is critical for understanding potential career fields as not all cybersecurity personnel are required to be proficient to the same level of technical understanding. Cybersecurity technicians specialize in technical skills, while cybersecurity personnel can have either technical or non-technical skills [17]. Examples of these variations may include, a cybersecurity technician could be someone who specializes in firewall operations, while a cybersecurity personnel member may be someone who specializes in cyberpsychology. Skills required for each career field within cybersecurity often take years to hone, even to a satisfactory level. Technicians develop softer skills through a quasi-apprenticeship, such as skills developed in psychology, sales and

marketing, law enforcement, intelligence, risk management, project management, or other people-specific career fields.

2. Methodology

Informal education tends to be qualitative, experiential, and phenomenological, meaning it is interpretive for the individual experiencing and seeking the education [14][15][2]. Informal education is experiential in that there is no curriculum guiding the outcomes; individuals train until they feel they have mastered the subject, sometimes for professional certification, other times without it but the there is no structured outcome to train to. Formal education would be any education in which the outcomes are predetermined for students to reach. In this sense, experiences become phenomenological as the constructed experience becomes a localized phenomenon guiding the individual to study or learn more [14][15]. Finally, qualitative means the only measurement of the training effectiveness is the betterment of individual use or capability; generally, qualitative assessments are not measured against assessments other than the occasional professional certification [14][15].

Formal development of education tends to have measurable outcomes; therefore, it is quantifiable [2]. Educationally, developed courses such as curricula delivered either online or within a classroom with established outcomes would fall within this category. This paper will primarily deal with the formal education process versus the informal or experiential process, again without having the quantifiable outcomes associated with formal education no matter how the education is delivered.

Blue team members coordinate the organizational defensive posture, while red team members coordinate organizational offensive testing against internal targets [4][5]. A simple way to look at red and blue team members are red teams are typically technical auditors while blue team can be described as system or security administrators, for every task an administrator or manager performs an auditor will need to verify the task has been securely and efficiently. Red and blue teams will need to take actions to either reinforce or disable recognized countermeasures of people, processes, or technology [13][11].

3. Basic Cybersecurity Skills

Schools tend to focus on perspectives which are comfortable and easy to provide instructors for or answer a specific need within their community [3][4][5]. Schools could easily focus on remediating training by initiating individual concepts used in adjoining fields of study. Cybersecurity programs not encompassing all security countermeasures are countermeasure specific [13][11][3][4][5].

Academic institutions and professional organizations do not fully identify fields of study as cybersecurity other than fields traditionally associated with a chosen technology, or technology subcomponent as defined by IEEE or ACM, but this only encompasses three percent of the 2020 breaches as disclosed by IBM [10][17] [3][4][13][5][11]. A technology subcomponent may include a field of study such as a given technology auditing or training organizational employees to resist social engineering, which is typically classified as an information technology attack [3][4][5]. The remaining 98% of breaches occurred as either a direct or indirect result of a failed process or an interaction with a person; technologists would act as though this is a technology problem and not a security problem [20][10]

[17][3][4][13][5][11]. Early authors warned and continued to warn that security that only embraces a person, a process, or a technology is only a countermeasure for that person, process, or technology [13][11].

Special consideration to already developed skills immediately translatable to cybersecurity fields that align with those already identified by the individual task force quick implementation [3][4][5]. The cross-cutting concepts of integrity, confidentiality, availability, risk, adversarial thinking, and systems thinking intertwine content from these task forces [3][4][5]. The concepts of integrity, confidentiality, and availability were first established by J. McCumber and later reinforced as the basis for what is known as the CIA triad by Maconachy et al. [11][13]. The eight knowledge areas include human, organizational, societal, data, component, system, software, and connection [3][4][5]. Distributed knowledge areas exist in not only the six fields recognized by the computer curriculum 2020 task force [3].

4. Adjoining Cybersecurity Skills

Commonly identified cyber activity is technology-driven, but without understanding how people, processes, and technology interact as a single socio-technical system or an *STS*, technology is only technology-specific security which can be called technical component security [13][11][3][4][5][12]. STS is the name given to the view that a person interacting with a given piece of technology is a single work effort, meaning the technology requires the person and the person requires the technology to function [12]. People and processes need specific skills outside of technology; an understanding of how people engage technology is critical to fully understanding cybersecurity [13][11][3][4][5]. People skills are not unique to cybersecurity; technologists seldom work well with end-users as advisory boards and employers often have to train technicians in soft skills [17][3][4] [13][5][11].

Common fields of study to assist in developing people skills are psychology, sociology, humanities, accounting, and anthropology. Applied fields may include international relations, cultural studies, linguistics, criminal justice, law enforcement, HUMINT, intelligence, leadership, ethics, management, human resources, organizational policy, risk management, actuarial science, and sales and marketing. Many fields, such as criminal justice, psychology, linguistics, sociology, leadership, law enforcement, forensics, and management, have crossed the cyber realm. Fields such as ethics or risk management are often seen as topics contained within fields but are emerging as unique fields of studies within cybersecurity; using field specialists can increase the efficacy of cybersecurity personnel.

5. Sales and Marketing vs. Social Engineering

Sales and marketing involve invoking emotions to sell products or services to an end-user using the same marketing techniques and strategies which lead to developing a red team social engineer or a blue team training advocate. The primary purpose of marketing is to engage a consumer and get the consumer to purchase or engage in an activity that the customer normally would not do. Sales and marketing tactics compare to red team tactics such as social engineering, a tactic used to manipulate someone to do something they would not normally do, can be used as a defensive or blue team tactic to raise awareness for techniques to effectively train resistance against social engineering [18].

Countering social engineer techniques may include cyberHUMINT, cyberpsychology, applied training, sociology, cyberIntelligence, or even advanced cultural awareness and training operations [1][8][20]. CSEC 2017, CC 2020, or other presentations primarily focused on using technological methodologies to mitigate threats in the people countermeasures category, demonstrating limited abilities to identify threats [3][4][5]. Cybersecurity implementations primarily driven by technology will remain technically dependent; this is neither good nor bad, versus implementations driven by human factor development will be primarily driven by education and awareness [1][8][20][3][4][5].

6. Personal Skills Vs. Cyberpsychology

The Global Competency Model for Graduate Degree Program in Information Systems refers to "ethical and intercultural perspectives" which is a critical component of understanding the human perspectives on a problem but commits very little explanation or effort to understand it [19][3]. ACM covers very little regarding the human perspectives; it leaves skills used to study people to specializations trained in soft skills, including communications, behaviors, and interactions [19][3][4][5]. Psychologists, sociologists, anthropologists, international relations, cultural studies, linguistics, criminal justice, law enforcement, HUMINT, intelligence, leadership, ethics, management, human resources, and sales and marketing are commonly identified as containing an emphasis on the study of people and how they interact with their environments. Integrating specialists who study people provides an opportunity to cross-train these skilled specialists into a technical awareness and thus produce a new type of specialist capable of enhanced working with the people component of people, processes, and technology. The inverse of this, using these specialists to train cybersecurity personnel and technicians increases the efficacy of cybersecurity personnel and technicians as they address the people countermeasure concerns in the workplace.

7. Unorthodox Training of Analysts and Strategists

Cybersecurity analysts, which O-Net or the US Department of Labor may address as information security analysts or associated job codes encompass CIP code 15-1212.00 or other adjoining CIP codes such as CIP 11.1003 as defined by the US Department of Education [21][22]. Cybersecurity and security analysts and are very difficult to train as analysts have to train to view a more extensive picture capability yet see the individual components of the picture seeing relationships between objects [21]. CIP or classification of instructional codes are groupings of skills that are aligned and found to be common to a given skill or technical profession [22]. The analytical skills are almost impossible to train. Many cybersecurity personnel enjoy cooking or creating music; oddly enough, the skills for creating music or cooking mirror the skills needed for cybersecurity analysis, analysts have to have the ability to see the interconnectedness of components [7]. Clifton strength finders typically call these skills *connectivity* and *individualism* [7].

8. Physical Security Engineering

Physical access to a system is an open invitation to disaster or attack. Nevertheless, training such as Crime Prevention through Environmental Design or *CPTED*, as described in the International Standards Organization 22341, is often reserved for either architects or

physical security experts (International Standards Organization, 2021; [6]). Physical threat analysis is practiced by law enforcement, criminal justice, emergency management, security practitioners, and personal security personnel; it is a key tenant of data protection [19][3][4]. Data security personnel may not be the most appropriate to train cybersecurity personnel in physical security.

9. Conclusion

Cybersecurity continues to expand to fields of countermeasure study outside of technology and processes, yet few attempts to better understand the people countermeasure have been made. Technology countermeasure specialists in ACM and IEEE recognize they are ill-prepared to counter issues that deal with complicated processes or people countermeasures. Specialists in individual countermeasure techniques should be engaged and integrated to provide better guidance in various fields of study, specifically in the people and process countermeasures.

References

[1] S. Back and J. LaPrade, (2019). The future of cybercrime prevention strategies: Human factors and a holistic approach to cyber intelligence. International Journal of Cybersecurity Intelligence & Cybercrime, 2(2), pp. 1-4. [Online] Available: https://www.doi.org/10.52306/02020119KDHZ8339

[2] J. W. Creswell and J. D. Creswell, (2022). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches 5th Edition. p. 50.

[3] CC 2020 Task Force. "Computing curricula 2020: Paradigms for global computing education," Association for Computing Machinery, New York, NY, USA. 2020. pp. 50. [Online] Available: https://doi.org/10.1145/3467967

[4] Joint Task Force on Cybersecurity Education. "Cybersecurity curricula 2017: Curriculum guidelines for post-secondary degree programs in cybersecurity," Association for Computing Machinery, New York, NY, USA. 2018. [Online] Available: https://doi.org/10.1145/3184594

[5] Cyber2yr2020 Task Group. (2020). Cybersecurity curricular guidance for associate-degree programs. Association for Computing Machinery, New York, NY, USA. [Online] Available: http://dx.doi.org/10.1145/3381686

[6] European Commission Directorate-General Justice, Freedom, and Security. (2005). Planning urban design and management for crime prevention handbook. costtu1203.eu/wp-content/uploads/2014/10/Handbook-English.pdf

[7] Gallup. (2007). Strengthfinder 2.0. Gallup Press. [Online] Available: https://www.gallup.com/cliftonstrengths/en/253715/34-cliftonstrengths-themes.aspx

[8] C. Hadnagy, (2010). Social engineering: The art of Human Hacking. Indianapolis, Indiana; Wiley Publishing Inc., 2001

[9] *Security and resilience; Protective security - Guidelines for crime prevention through environmental design*, ISO 22341:2021

[10] IBM Security. (2021). Cost of a Data Breach Report 2020. [Online] Available: https://www.ibm.com/security/services

[11] W.V. Maconachy, C.D. Schou, D. Ragsdale, and D. Welch, "A model for information assurance: An integrated approach" *Proceedings of the 2001 IEEE Workshop on Information Assurance and Security*, ed. W.V. Maconachy, pp. 306-310, 2001.

[12] M. Malatji, V.S. Sune, and A. Marnewick. Socio-technical systems cybersecurity framework. *Information and Computer Security, 2019. 27*(2), 233-272. [Online] Available: http://dx.doi.org/10.1108/ICS-03-2018-0031

[13] J.R. McCumber. "Information systems security: A comprehensive model", *Proceedings of the 14th National Computer Security Conference.* National Institute of Standards and Technology. Baltimore, MD. October 1991, pp. 1-6.

[14] C. Moustakas, *Heuristic Research: Design, Methodology, and Applications 1st Edition.* London; Sage Publications, Inc. 1990. pp.

[15] C. Moustakas, *Phenomenological Research Methods 1st Edition*. London; Sage Publications, Inc. 1994. pp.

[16] A. Parrish, J. Impagliazzo, R. K. Raj, H. Santos, M. R. Asghar, A. Jøsang, T. Pereira, and E. Stavrou. "Global perspectives on cybersecurity education for 2030: A case for a meta-discipline." *In Proceedings Companion of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education (ITiCSE '18 Companion)*, July 2–4, 2018, Larnaca, Cyprus. ACM, New York, NY, USA, 2018. 19 pages. [Online] Available: https://doi.org/10.1145/3293881.3295778

[17] C. Paulsen and R. Byers, *Glossary of key information security terms (NISTIR 7298 Revision 3).* 2019. [Online] Available: https://doi.org/10.6028/NIST.IR.7298r3

[18] D. Strom, (2022). Red vs. blue vs. purple teams: How to run an effective exercise. CSO [Online] Available: https://www.csoonline.com/article/3647316/red-vs-blue-vs-purple-teams-how-to-run-an-effective-exercise.html

[19] The Joint ACM/AIS MSIS 2016 Task Force. "Msis 2016 global competency model for graduate degree programs in information systems," Association for Computing Machinery, New York, NY, USA. 2016. pp. [Online] Available: https://doi.org/10.1145/3127597

[20] E. Tuorinsky, *The human factor in cybersecurity: Overcome human nature with a lock the door mentality.* September 2021. [Online] Available: https://www.securitymagazine.com/articles/96009-the-human-factor-in-cybersecurity

[21] ONET Online. Information security analysts (CIP code 15-1212.00). [Online] Available: https://www.onetonline.org/link/custom/15-1212.00

[22] National Center of Education Statistics. CIP: The classification of instructional programs ONET Online. Detail for CIP Code 11.1003. [Online] Available: https://nces.ed.gov/ipeds/cipcode/cipdetail.aspx?y=55&cip=11.1003

