Leo Zhang

6/29/2022

IDC 6601

Assignment II

Cyber-HF-M&S Venn Diagram Discussion

Abstract

The venn diagram taught in class is a critical piece that make up the different aspects of modeling and simulation of behavioral cybersecurity. There are three main parts. There's the modeling and simulation, cybersecurity, and, the one I will expand upon, human factors. This is not to say that human factors is the most important. I think they're all equally important but I human factors is more easily applicable to a wider spectrum of users, including those with little to no knowledge of cybersecurity. I will also discuss any potential changes that should be imposed on this venn diagram.

Discussion

As shown there are three intersection areas. First we have behavioral aspects of modeling and simulation, which is the intersection between M&S and HF and includes training and performance, interdisciplinary methods for problem solving, cognitive modeling, and HSI. Training and performance can include topics such as receiving education to become more aware of potential scams and threats. Interdisciplinary methods for problem solving, which is an approach that critically analyzes the relevant disciplinary insights and attempts to produce a more comprehensive understanding or propose a holistic solution [1]. Cognitive modeling is a computational model that hinges upon psychological notions, demonstrating how people go about problem-solving and performing tasks [2]. Human system interface (HSI) is similar to human machine interface and, as explained in this article, is the most vulnerable element of an IT system. HMI refers to a dashboard or screen used to control or monitor machinery, either on-site or remotely. As the primary user interface for controlling equipment or a process, the HMI is among the most targeted aspects of the industrial control system (ICS) infrastructure. Unauthorized access to the HMI can cause havoc: operators can lose the ability to control a process; the breach can lead to asset damage and destruction; and in extreme cases, the incident can result in equipment injuries or even loss of life, during maintenance [3].

The second intersection is cybersecurity for M&S. This one includes cyber ranges, anomaly detection, OS modeling, and attack vector simulation. Cyber ranges are controlled, interactive technology environments where up-and-coming cybersecurity professionals can learn how to detect and mitigate cyber attacks using the same kind of equipment they will have on the job [4]. Anomaly detection which is using advanced data mining techniques to figure out what is being attacked as mentioned by the professor of this course. A more literal definition mentioned from an online article is the "identification of rare occurrences, items, or events of concern due to their differing characteristics from the majority of the processed data," allows organizations to track "security errors, structural defects and even bank fraud" [5]. An attack vector is a pathway or method used by a hacker to illegally access a network or computer in an attempt to exploit system vulnerabilities. Hackers use numerous attack vectors to launch attacks that take advantage of system weaknesses, cause a data breach, or steal login credentials. Such methods include sharing malware and viruses, malicious email attachments and web links, pop-up windows, and instant messages that involve the attacker duping an employee or individual user [6]. The simulation of this is done by many companies out there as a means of bringing about awareness to its employees of potential scams and attacks by malicious hackers.

The third intersection is the behavioral aspects of cybersecurity.This includes insider threat detection, cyber workforce development, attack prediction, and hacker motivations. Building a strong cyber workforce can better equip organizations with the tools and knowledge to counter cyber attacks and the other three points mentioned for this intersection. This is also the section I want to expand on because I think human factors are very important in the field of cybersecurity since the difference between falling victim to a cyber attack and countering it can be completely decided by one's decision making. Everyone has to make decisions on a daily-basis. It can be as simple as "what do I do today", "when do I do it", or "what should I prioritize". Human factors are also more applicable to a wider array of the audience. The intuition of the individual is greatly influenced by the person's past experiences, education, and trainining, which is why I believe the "training & performance" feature of the behavioral aspects of M&S should also belong in this third intersection as well. Another reason for my belief is that perceiving the four features of this third intersection is heavily influenced by decent training and so training should not be overlooked for this intersection. This article mentions that "an organization’s own personnel are an invaluable resource to observe behaviors of concern, as are those who are close to an individual, such as family, friends, and co-workers. People within the organization will often understand an individual’s life events and related stressors, and may be able to put concerning behaviors into context” [7]. As mentioned, detecting and identifying potential insider threats requires both human and technological elements. Vulnerabilities can also be detected through technology employed in conjunction with human sensors to detect and prevent insider threats. The article also mentions that an organization’s personnel are the human component for the detection and identification of an insider threat. Co-workers, peers, friends, neighbors, family members, or casual observers are frequently positioned for insight into and awareness of predispositions, stressors, and behaviors of an insider who may be considering malicious acts [7]. An example would be what the professor mentioned in class with companies sending out fake cyber attacks to their employees to see how many would fall for those attacks and to educate those who do fall for them so that they would be better equipped for the real attacks.

Conclusion

All three intersections definitely have their place to contribute in the field of M&S of behavioral cyber security. However I believe the behavioral aspects of cybersecurity is the most applicable to more of the common people. The features mentioned are all related to one another. For example, if employees at a company are trained properly to predict attackers, then they probably would have to come across acknowledging the attackers’ motivations. And with training the employees may have received most likely isn’t limited to the companies’ training, but also may include prior experiences, witnesses, education and basic common sense. However in the companies’ best interest the insider threat detection concepts are probably the most important because former and current employees have easier access to their own companies’ data and may cause either accidental or malicious damage [8].

[1] https://www.byui.edu/interdisciplinary-studies/solving-complex-problems
[2] https://www.interaction-design.org/literature/topics/cognitive-modeling
[3] https://www.xylem.com/en-us/making-waves/water-utilities-news/cybersecurity-series-human-machine-interface-hmi-or-hacker-machine-interface/
[4] https://cybersecurityguide.org/resources/cyber-ranges/
[5] https://securityboulevard.com/2021/07/what-is-anomaly-detection-in-cybersecurity/
[6] https://www.fortinet.com/resources/cyberglossary/attack-vector
[7] https://www.cisa.gov/detecting-and-identifying-insider-threats
[8] http://solidsystemsllc.com/insider-threat-detection/