Understanding the Most Effective Cybersecurity Techniques and Methodologies

Christopher Hossele

Old Dominion University

IDS 300W

Professor Patricia Oliver

December 8th, 2023

Cybersecurity is a subfield of information technology as a whole and focuses on ideas of protecting and securing an organization's assets through predictive knowledge and combative action. Cybersecurity involves years of policy creation and innovation, deriving the best steps to achieve successful security environments. Techniques that secure information involve physical system architectural formulas and the observation and management of human behaviors. The best products of achieving these results involve careful research through years of critiquing, observation, and innovation stemming from past flaws and discoveries. Approaching the best results can be done through an interdisciplinary perspective through the utilization of different disciplines and their evidence that is derived from literature works such as journals and other forms of documentation. With an interdisciplinary approach, it is beneficial to identify the disciplines that are used holistically to curate the conclusion of effective cybersecurity methods and practices which would be psychology, history, and information technology. These disciplines have the highest relevance regarding answering the question of what the effective methods of cybersecurity could be and the results from these perspectives are the most effective approaches through an interdisciplinary perspective. To be able to effectively identify these methods and practices individuals must understand the factors that support the achievement of common ground. Information technology as a discipline identifies itself as the study of computational environments, infrastructure, tools, techniques, and human contribution to the world of computer technology. The research of information technology systems and past cyberattacks supports the objectives of identifying the most effective methods of strong cybersecurity mitigation and infrastructure, being able to understand the most prominent reasons as to why issues occur. When it comes to identifying these reasons, human contribution is the

biggest component to the attacks and/or negligence of cybersecurity systems. The study of psychology as a discipline imposes a perspective of why these threats occur to cybersecurity systems and analyzes human behavior that underlines the reasonings. Looking at it through this perspective helps understand human factorial causes of vulnerabilities and threats through the study and analysis of past events that involved human error, supporting the reasonable utilization of psychological research. Since the creation of digital technology and the integration into societal routines, psychology has been expanded more into the most effective mitigation methods and procedures that have shaped strong cybersecurity policies over the years. This can involve proper employee training and using behavioral patterns to mitigate outside threats with a short arm of predictive knowledge approach. The perspective of history helps study the past patterns and historic significant events that support effective methods and practices through a chronological structure of influence and innovation. Being able to understand a timeline of events and discoveries that foreshadow the change of policy and physical systems helps further an understanding of how cyber professionals learn from former discoveries. The integration of history using the evidence of past significant events of psychological study helps develop a conclusion of effective practices and methods of cybersecurity. Considering the past helps impact the future. Through these lenses of integration, it allows for creating common ground among the disciplines and helps support a strong conclusion of proper cybersecurity. The drastically advancing technologies that significantly impact society continue to develop and change through the lens of the most effective methods and practices and will forever be shaped by further research. The question of what the most effective methods and practices of

cybersecurity are can be developed through the perspectives of psychology, information technology, and history disciplines.

Like other forms of peak engineering methodology, consistent advancements of cybersecurity infrastructure throughout the years were inaugurated using history. These momentous events involved the education of solution discovery stemming from cyberattacks and other forms of vulnerability throughout the years. It wasn't until the 1980's when cybersecurity became a known terminology as "cyber espionage." This allowed for further research and development to eventually begin creating guidelines for computer environments, later coining the terminology "cybersecurity" as a field of study preceding the years of research and discovery. The consistent cyber-attacks that emerged in the 1980's influenced a broader spectrum of research to create better and more efficient guidelines. From the initial set of cyberattacks, the Department of Defense implemented the "Trusted Computer System Evaluation Criteria" as a basis for information technology processes (Aslan, 2018). This meant that human contributions had to take a step forward, allowing employees to familiarize themselves with new concepts and regulations to prevent future cyberattacks. The history of cyberattacks did not stop here of course, as new techniques that hackers curated would continue to dismantle cyber systems (Aslan, 2018). With this, information technology environments had no choice but to advance themselves as the threats advanced too. The majority of these cyberattacks committed throughout the past only fueled the fire to innovate the future techniques of security, as software security was released in the late 80's and Secure Sockets Layer (SSL) was introduced in the mid 90's (Aslan, 2018). The concern for security began to grow more as

technology advanced throughout society, causing people to quickly fear the results of cyberattacks. The integration of psychology helps identify some key components to these reactions of cybersecurity history. The Psychological toll cyberattacks impacted on society only motivated information technology professionals to create better security protocols. Apart from discovering effective advancements in information security came the need for proper employee training.

Psychology, specifically social psychology, is a key component of achieving the level of having effective cybersecurity methods and practices. Psychology as a discipline is the study of human characteristics in relation to evidence gathered from analysis and patterns of human behavior (Reber, 2019). In cybersecurity, human behavioral patterns foreshadow successful innovations and when partnered with the perspective of psychology, a formation of proper mitigation techniques occurs and are centered around the environment of information technology (Dreibelbis, R 2018). In this perspective, psychological factors within an information security workplace involve proper employee education, training, and management (King, Z 2018). Social engineering is a substantial portion of psychology in relation to cybersecurity. Social engineering regarding information technology can be identified as "the use of deception in order to induce a person to divulge private information or esp. unwittingly provide unauthorized access to a computer system or network." (Hatfield, 2017). This influences the creation of certain policies and procedures that support the mitigation of future anomalies that can lead to potential vulnerabilities and threats, migrating away from falling victim to social engineering attacks. There are many forms of social engineering that influence the impacts of cyberattacks, such as phishing or spear phishing.

Phishing attacks are a form of psychological weapon that utilizes social engineering to exploit information. The attacks are carried out by individuals who impersonate positions that can easily be falsely recognized as reputable, typically posing as a family member, employer, organization, or trusted bank that is commonly used. Typically, phishing scams can happen in the form of emails, text messages, or phone calls and can deceive people into giving out their personal information to individuals who would want to steal their assets, such as bank information (Aleroud, 2017). The scams that are sent to people are made to look authentic and aim to deceive individuals into giving their information through persuasion. Spear Phishing is a sub-phenomenon of phishing that involves an employment setting in which attackers trying to gain access to information within systems will mimic as information technology departments or higher position officials to gather company information and security information. Typically, these are harder to identify compared to normal phishing scams and usually develop over a long duration of time before being carried out. (*What is Social Engineering*). To mitigate spear phishing tactics, cyber professionals suggest confirming the source with the individual that it pertains to. Cybersecurity professionals typically implement multi-factor authentication into their systems and ensure that this information is never asked over the phone or any other forms of communication. Proper employee training helps recede the threats of psychological weapons being used within cyber-attacks, giving employees the ability to educate themselves about proper policy guidelines and particular social engineering tactics that are used against them. These policy structures have developed throughout the history of cybersecurity as more forms of social engineering attacks occur, garnering the motive to ensure vigorous training practices for employees.

The perspective of information technology and its influence helps support the idea of the most effective cybersecurity techniques and methodologies. Information technology gives specific tools and environments such as software, hardware, firewalls, and other forms of physical technology that would be considered information technology (Kim, S). There are also a fair share of rules, regulations, and guidelines that revolve around the concept of information technology. These designs and guidelines were curated using the most efficient practices and methodology through experience and research (De Vaujany, 2018). Integrating the use of psychological research helps influence the creation of these practices and methodology by understanding how psychology conforms to the practices of cybersecurity. Cybersecurity professionals use psychology as a forefront to prevent cyberattacks from occurring and implement this into its architecture and regulations. For example, the NIST Framework is a standard of the most effective cybersecurity practices and guidelines. These guidelines were created using an interdisciplinary approach such as the use of psychology to help regulate the cybersecurity environments. Integrating psychology and information technology together helps create these strong methodological theories.

Looking back at the years of expertise regarding the innovations of cybersecurity techniques and practices, it shows how much psychology and history affect the decision-making process of the peak effectiveness of certain fields. Interdisciplinary approaches for securing common ground for a particular dilemma through psychology, history, and information technology are crucial to understanding an affective concept. Cybersecurity involves years of policy creation and innovation, deriving the best steps to achieve successful security environments and have shown this evidence thoroughly through the disciplines. Empowering the

ability to educate about certain historic events that have influenced the change of cybersecurity policies helps understand the most effective techniques within present time. The psychological factors of these paired with historical moments through a holistic viewpoint significantly support the findings that lead to understanding the most effective concepts of information technology cybersecurity.

References

1. King, Z., Henshel, D., Flora, L., Cains, M., Hoffman, B., & Sample, C. (2018).

Characterizing and Measuring Maliciousness for Cybersecurity Risk Assessment.

Frontiers in Psychology

2. Dreibelbis, R., Martin, J., Coovert, M., & Dorsey, D. (2018). The Looming Cybersecurity

Crisis and What It Means for the Practice of Industrial and Organizational Psychology.

Industrial and Organizational Psychology

3. Aslan, &., Aktuğ, S., Ozkan-Okay, M., Yilmaz, A., & Akin, E. (2023). A Comprehensive

Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. Electronics (Basel)

4. De Vaujany, F., Fomin, V., Haefliger, S., & Lyytinen, K. (2018). Rules, Practices, and

Information Technology: A Trifecta of Organizational Regulation. Information Systems

Research

5. Kim, S., Kim, B., & Seo, M. (2020). Impacts of Sustainable Information Technology

Capabilities on Information Security Assimilation: The Moderating Effects of

Policy—Technology Balance. Sustainability (Basel, Switzerland)

6. Reber, Rolf. 2019, Psychology [e-Book]

7. Aleroud, Ahmed, and Lina Zhou. “Phishing Environments, Techniques, and Countermeasures:

A Survey.” Computers & Security, vol. 68, 2017, pp. 160–196.

8. *What is Social Engineering: Attack Techniques & Prevention Methods: Imperva*. Learning Center. (2023, March 14). https://www.imperva.com/learn/application-security/socialhttps://www.imperva.com/learn/application-security/social-engineering-attack/engineering-attack/