Unraveling Human Behaviors in Cybersecurity for Enhanced Information System Defense:

Old Dominion University

IDS 300W: Interdisciplinary Theory and Concepts

Camryn Patillo

November 26, 2023

Abstract Page

In this interdisciplinary paper, I will discuss human behaviors in cybersecurity and how we could provide better defensive security for information technology. This paper seeks to navigate through the complexities of human behavior in the cybersecurity domain, drawing insights from psychological frameworks to decipher decision-making processes and cognitive biases that influence security postures. Concurrently, it will explore the social sciences, unraveling the fabric of organizational cultures and their impact on information security practices in the business space. In recent times, there has been a surge in technological advancements that has shown some extraordinary improvements in our society and has brought a wider variety of opportunities for not just individuals but for the country as a whole. By now it is common knowledge that as the landscape of information technology expands, the necessity to strengthen our cybersecurity defenses becomes increasingly paramount. As I explore the concepts of behavioral theories, my goal is to develop an understanding of proper training that can be implemented in our information systems and security. Using the disciplines of information technology, psychology, social sciences, business, and law; I hope to not only find improvements in the common security programs by exploring their defensive capabilities, but I also hope to explore potential chances to create a common understanding among individuals. This will help the overall awareness of information technology and foster a resilient society.

Since the boom of the internet in the late 90s, the internet has been in a constant state of rapid growth. Compared to the beginning, the internet has grown so much it is a staple tool that is utilized by millions of people. The internet is also used so much, that our society has adapted to it as a second living environment where people can communicate, sell, buy, and profit without any need for physical interactions. While all these are life-changing, running a business, buying items, and sharing personal information is less safe physically than it is online. In fact, it is safe to argue that chronic online exchanges can even be dangerous. While the internet continues to grow, individuals and businesses need to develop an interdisciplinary perspective on the matter to keep it safe.

As we witness the persistent growth of technology, a very important question to ask is who is responsible for keeping the internet safe? According to Norton LifeLock, the responsibility leads to a complex collective responsibility between government officials, individual internet users, and corporations (Norton LifeLock, 2020). But how are we as a society able to effectively provide systems of protection without finding a common ground amongst the different groups of people we deem responsible for it. It is important to use interdisciplinary skills to figure out these conflicts.

An interdisciplinary perspective will become a critical tool for finding an effective solution to this question. First, it is important to establish what the conspecr of information systems and information technology is and how it relates to cybersecurity.

Information systems can be described as cohesive sets of elements designed to collect, store, process data, and provide information (Zwass, 2023). From an interdisciplinary perspective, the concept of information systems will be useful in understanding the technicalities

of what it takes to protect it. The main components that are used to protect information systems include firewalls (internal network security systems), data encryption (ensures confidentiality, transmitted through multiple networks), and authentication (fingerprints, username/password, smartcards, etc) (Zwass, 2023). Notice, that the traditional expectations of a well-rounded secured network system are mostly hardware and software-based. Humans are hardly recognized as an important factor in the security process regarding information systems.

A popular and common argument against relying on humans to protect information systems is due to the differences in the rate of error between humans and technology. In fact, it is said that 88% of data breaches are caused by human error (CYDEF, 2021). While technology does malfunction and commit errors, the rate is far less than the error of human labor. In the article "The Human Factor: The Hidden Problem of Cybersecurity," by CYDEF the opposing viewpoint of humans protecting information is discussed. It stated that 57% of employees claimed they are more distracted while working in an environment that requires more productivity and attention (CYDEF, 2021). This is why I think that applying interdisciplinary skills is extremely important even when it seems ineffective.

I believe that most should consider relying on human security because it has its advantages when it comes to analyzing the human behavior and psychology behind cybercriminals and hackers. These kinds of analytical abilities are extremely important in the field of cybersecurity when protecting information systems.

Behavior psychology principles in the field of security prove their significance when applying effective security programs to increase the defensive qualities of businesses and/or corporations' information systems. It can also be useful in developing strategies to leverage the cognition of cybercriminals and hackers. From a business perspective, applying behavioral

psychology principles to cybersecurity and information security can benefit the quality of surveillance and defensive approaches employees will make. In the article “Why cyberpsychology is such an important part of effective cybersecurity,” by Mary K. Pratt, it is stated that CISOs (Chief Information Security Officer) can greatly benefit from cyberpsychogists despite the shortages. Understanding the cognition processes of hackers such as decision-making processes or motives, can give a company under security breach leverage against a cybercriminal (Pratt, 2023).

An example of using psychological tactics to gain leverage on computer systems over an opponent is social engineering. Social engineering is a psychological technique both hackers and cybersecurity employees use. Social engineering can be explained as using digital equipment or contact to gain access to information. For example, hackers will use phishing or phone spamming to gain illegal access to either an individual or an organization’s information systems (KnowBe4, n.d). When employees use social engineering to protect information systems, they tend to do it with the honeypot method. It is a method in which those who are trying to catch cybercriminals by creating a false computer system made to attract hackers and cybercriminals. With this technique, employees and the human intelligence sector of a company will analyze the human behaviors the hackers will take part in on the computer server. With this, they use these behaviors hackers showcase on the system to predict and prevent future security breaches (Kaspersky, n.d).

Using Interdisciplinary techniques will also lead to human behavior and Information technology from a business perspective. Relying on employee training instead of investing in new security technology and software can be proven to be more cost-efficient (Florentine, 2018). Employees will evoke human behaviors such as natural competitiveness, curiosity, and

engagement to improve their knowledge of the security of information technology. And this will save companies and corporations money on not just equipment, but it will also save the money they would need to spend if a security breach decimated sensitive information such as invoices, data-encryptions, etc.

Nowadays, businesses are looking into more Risk Management positions because people are realizing the better alternatives to combating the dangers of technology growth are human labor and resources. It also provides companies and corporations with a better defensive quality by finding fault with any of the data systems of a company (SafetyCulture, 2023). The five main management tools according to ScafetyCulture, are SWOT (Strengths, Weaknesses, Opportunities, and Threats), Root Cause Analysis (method of problem-solving), Risk Register (identification of potential risks for a company), Probability and Impact Matrix (prioritization of risks), and Brainstorming (assessing insights of external factors) (SafteyCulture, 2023). Most of these methods could not by done with machinery, it would take a team of *people* to achieve good quality risk assessment and management to protect many assets of a business organization. One of those being information systems. A company's system is one of the most important factors of an organization to keep safe.

This is why most companies and corporations heavily rely on employees to make sure they are following secuirty protocols in order to effectively keep information and data safe. This could be by coming up with complex passwords, two-step authentication, fingerprints, etc. When adding in the psychological perspective, one could argue that human beings will not be able to provide an up-keep on these behaviors. This is why it is important to enforce such rules and regulations within a business or organization. It is important to enforce such rules even in regular society and not just within a business or organization.

While considering the legal perspective of protecting information technology, legal frameworks for information systems is critical in establishing accountability and discouraging malicious activity through technology. The ability to take accountability in a workplace can only improve the quality of work that is being done. When an employee breaks an enforced rule to improve security systems to protect a company's information system. It is a responsibility of an employee to own up to their mistakes. Even the mistake was a simple human error, taking accountability will only show improvements in the quality of work the individual will provide, but it will also feed into other employees as well when an example has been made. Once again, going back to the psychological perspective, according to the organization "Torch", accountability can show improvements in all employees. This is because employees taking accountability as shown to build trust amongst each other, strengthen relationships, and minimize future mistakes from occurring (Torch, 2021).

Legal Implications and Compliences can be proven useful when trying to use human behavior as an advantage. The Deterrence method is a criminal justice technique used by lawmakers to use legal regulations to prevent further malicious behavior from growing. This is an example on how analyzing human behavior can be useful in enforcing laws. And by following these laws, individuals and organizations are actively playing a hand at decreasing the rate of cybercrime not just in businesses and corporations, but this could be useful in solving and preventing cybercrimes and security breaches for society's benefit. In short, the results are more long-term when relying on human behavior and labor to protect information systems rather than solely relying on technology and various forms of automation and encryptions.

Social sciences should be more applied to cyber security techniques to improve defensive capabilities on information systems. It allows cyber-specializes to proper consider the human and

behavioral aspects and patterns a cybercriminal can make. It also allows more room for cyber-specialists to apply more interdisciplinary studies and skills to investigations, analysis, and defense of an individual or business's systems. By applying insights such as psychology, business, social sciences, etc, professionals will come to realize they have a lot more to offer when considering the benefits of analyzing and applying human behavior techniques

Of course, it is safe to acknowledge the pros and cons of prioritizing human labor instead of technology. Humans will never have the ability of consistency in the way the technology is able to perform it. And as it advances, technology will also outside human labor in efficiency and sometimes quality. However, I believe that technology only does good at solving problems in a short-term sense and it will be incapable of using human skills such as interdisciplinary study to serve its purpose with a long-term solution. This is something human labor will always excel in compared to technology and computers. When considering the effectiveness of human behavior, there is so much to solve and conquer, but when delving into insights of psychology, business, and social sciences, it can be turned into something that was once viewed as a liability into and an advantage. Applying these techniques to security protocols, legal frameworks, and defensive techniques for information systems, will allow our society to get used to a more effective solution to the use gap between technology evolution and the danger it comes with and human skills and behaviors.

In conclusion, human behavior is a key factor in cybersecurity training and the protection of information technology. I've explored the integration of psychology, social sciences, business, and law enforcement and how it can have an impact on improving technological security. And I've explored the potential dangers it could bring as well. Exploring the psychological, behavioral, and social concepts of the research, it gave a better understanding of human

behaviors and how to prevent it is when it comes to basic security. It also proved that understanding human behaviors can be used as an advantage when it comes to preventing potential security breaches or cyber-hacking. This understanding can be applied to the concepts of business and how understanding human emotions and behaviors can benefit organizations. By providing more training for employees, a company training system can possibly weaponize human intelligence to protect information systems and provide proper security for data. A great understanding of human behavior can also prove useful to law enforcement by understanding the motives of cyber-hackers, studying the everyday behavior of cyber-hackers, and understanding social engineering tactics so they can be prevented.

Essentially, integrating insights into psychology, business, social sciences, information technology, and law all help measure a comprehensive understanding of human behavior and the amount of benefits it has on many different sectors of information systems if it is allowed to be utilized to provide proper security tactics (U.S. Department of Justice, 2016). This also supports my argument from a psychological perspective point of view. That analysis of criminals' social and human behavior can be useful in figuring out how to solve or prevent a crime. This also applies to cybersecurity and protecting information systems. If there are regulations that are being enforced, fewer people will likely commit cybercrimes due to hackers and potential cybercriminals not wanting to suffer any consequences.

Reference

CYDEF. (2021, May 19). The Human Factor: The Hidden Problem of Cybersecurity. Retrieved from https://cydef.ca/blog/the-human-factor-the-hidden-problem-of-cybersecurity/

Florentine, S. (2018, December 21). IT training: The most effective options for upskilling IT staff. CIO. https://www.cio.com/article/222632/it-training-the-most-effective-options-for-upskilling-it-staff.html

Kaspersky. (n.d.). What is a Honeypot? https://usa.kaspersky.com/resource-center/threats/what-is-a-honeypot

KnowBe4. (n.d.). What is Social Engineering? https://www.knowbe4.com/what-is-social-engineering/

NortonLifeLock. (2020, March 30). Who's most responsible for your data privacy protection? Government? Companies? You? *TechCrunch*. https://techcrunch.com/sponsor/nortonlifelock/whos-most-responsible-for-your-data-privacy-protection-government-companies-you/

Pratt, M. K. (2023, July 4). Why cyberpsychology is such an important part of effective cybersecurity. CSO Online. https://www.csoonline.com/article/643967/why-cyberpsychology-is-such-an-important-part-of-effective-cybersecurity.html

SafetyCulture. (2023, November 11). Why Risk Management is Important for Organizations. https://safetyculture.com/topics/risk-management/#:~:text=Simply%20put%2C%20risk%20management%20aims,reputation%2C%20or%20harm%20to%20employees.

Torch. (2021, March 10). How Accountability Leads to Successful Management. Torch.io. https://torch.io/blog/how-accountability-leads-to-success/

U.S. Department of Justice. (2016, June 5). Five Things About Deterrence. National Institute of

Justice. https://nij.ojp.gov/topics/articles/five-things-about-deterrence

Zwass, V. (2023, November 10). Information System. Britannica.

https://www.britannica.com/topic/information-system