More Than the Ghost in the Shell

A Discourse on the Human Factor in Cybersecurity

Jayden Dorey

CYSE 200T

Professor Kirkpatrick

27 September 2026

Definition

While cybersecurity has no place without technology and hardware, the human factor is a facet of the field that requires more attention as the root of both cybersecurity and cybercrime. The "human factor" in the field could loosely be defined as the nature of the human users of technology and how their behaviors impact the use of that technology. On a more robust level, it is defined as the "individual human behaviors and the social structures that enable collective action by groups" through the use of technology (Dupont & Holt, 2021). In other words, the human factor relates to the non-technical aspects of users, such as motivations, psychology, and sociology. Because attributes rely on fields that reach outside the traditionally recognized scope of cybersecurity, they are not as talked about, leaving this factor open for vulnerabilities. The more we, as a field, begin to dive deeper into the individual "behind the screen," the better we can plan and respond to attacks. Just as ambiguous as human nature is, so should the field of cybersecurity be.

Contribution to Vulnerabilities and Incidents

The human factor is arguably the most vulnerable aspect of the field because of the variety of factors that make up a single individual and their way of thinking. In the context of vulnerabilities, the simple act of recognition differs from one person to the next; what one person might see as a plain and imminent threat, another might completely disregard as anything out of the ordinary. This relative judgment is a large part of the justification when it comes to cybersecurity awareness and education in the workplace. These mandatory training sessions provide a baseline for the creation of mindsets in individuals who are potentially exposed to threats on a regular basis. Regardless of the breadth and depth of training, the fundamental decision-making aspect relies more on the individual and a plethora of factors, most pertaining to

their specific psychology. In this way, social engineering offers attackers the best opportunity to wrongfully obtain information of individuals who failed to recognize the malicious intent.

Examples

One example that demonstrates the correlation between human nature in the field is the prevalence and reaction to phishing attempts. Phishing is defined as an attack that tricks the user into providing the attacker with sensitive information, such as credentials or financial information (Kim & Solomon, 2023). These attacks work so well because they prey on the psychology of an individual and attempt to make them question their judgment based on the details in the message, the formatting of the message, or the alleged sender of the message. Specific types of phishing, called spear phishing, rely on gathering specific information about a target and then referencing that information to make the attempt more believable. Whaling is another type of spear phishing where the target usually holds a more executive role in a large company, making the information taken from them more valuable to the attacker and devastating for the company.

Another example that shows the relationship between the human factor and vulnerabilities is the prevalence of pharming. Pharming is defined as a specific threat in which the attacker is able to “obtain personal or private financial information through domain spoofing” (Kim & Solomon, 2023). This threat also involves DNS poisoning, an action in which the actor “poisons” a webpage so that when the user inputs the URL, it navigates them to a fake version of the website owned by the actor, allowing them to steal the credentials for the real website from the user (Kim & Solomon, 2023). This type of attack is difficult to spot by most because the website usually looks and functions identically. On the off chance that the website's

functionalities are not the same, most people would simply chalk it up to a connection error. This mindset is the human factor.

Reflection

The most common way to minimize the negative impact of the human factor in the field is through training and awareness. Like any other topic, the hope is that the more it is talked about, the more it will become engrained in the individual. In my experience, some companies have even started taking it a step further and creating their own social engineering scenarios and using those as educational tools. For example, once a quarter, Target will send out fake phishing emails to employees that have an internal account and work on the internal network for their position. If they open the email and interact with it, they are automatically directed to the training forum of the company and enrolled in a cybersecurity education course. This method of immediate cause and effect training is extremely beneficial because it not only provides supplemental training but also shows the employee how fast a threat can occur from one lapse in judgment.

Other than training, the culture of the workplace heavily shapes the mindset around cybersecurity. Though it might sound unnecessarily robust, treating every communication like a potential threat is often the best way to mitigate incidents. If every email received was considered as a threat initially until proven otherwise, the rise of successful attacks would decrease immensely.

Considerations

The psychology and background of an individual are only parts that make up the entirety of the human factor. These factors directly impact behavior and decision-making in the field of

cybersecurity. One specific aspect deals with the relationship and exposure the individual has to technology over the course of their life. For those that grew up with modern technology, the likelihood of a heightened awareness when it comes to threats and vulnerabilities is higher than individuals who had to learn about technology after entering the workforce or finishing their higher education. In this regard, it might be easier for those that grew up with a bottle in one hand and a tablet in the other to recognize these threats because they have been aware of them since childhood. On the other hand, those that grew up with limited access to technology are also limited on the exposure they had to technological vulnerabilities. Because of this, it is more difficult for them to recognize them as they present themselves, and for them to determine how to deal with them once they are made aware. While the argument is everpresent, being socialized with technology as a child should be considered and weighed just as traditional socialization is considered.

Conclusion

The human factor of cybersecurity is the piece of the field that fully realizes its interconnectivity with not only traditional STEM-adjacent fields, but the entirety of the educational universe. It also offers a method of understanding when it comes to cybercrime and their perpetration. The human factor is a collective of what makes the user a person, and how those attributes dictate their behaviors and actions in relation to technology. Without investing resources in understanding this factor, the field of cybersecurity will continue to have unpatched vulnerabilities at the hands of those they are trying to understand.

References

Dupont, B., & Holt, T. (2021, April 29). The Human Factor of Cybercrime. *Sage Journals*, *40*(4). https://journals.sagepub.com/doi/10.1177/08944393211011584

Kim, D., & Solomon, M. G. (2023). *Fundamentals of Information Systems Security* (Fourth ed.). Jones & Barlett Learning. https://reader2.yuzu.com/reader/books/9781284238815