The Human Factor in Cybersecurity

Andrew Judy

School of Cybersecurity, Old Dominion University

CYSE/IT 200T - Cybersecurity, Technology, & Society

Professor Chris Bowman

In cybersecurity, the human factor refers to the role that human behavior, psychology, and actions play in both compromising and protecting the overall security of an organization. This can include choosing to disclose confidential information about organization security, and creating weak or strong passwords. The human factor plays a key role in cybersecurity because if there is poor decision-making, or a lack of knowledge of social engineering tactics such as phishing, then cybersecurity is compromised as a result. This paper will examine how human behavior can contribute to cybersecurity vulnerabilities or incidents, identify and analyze at least two examples of cybersecurity risks related to human actions, discuss how organizations can reduce human-related cybersecurity risks through training, and consider how psychological, social, or organizational factors influence cybersecurity behavior and decision-making.

Human behavior can contribute to cybersecurity vulnerabilities and incidents because of a lack of carefulness in ensuring security at all times and negligence in properly maintaining systems such as not keeping systems up-to-date or updating credentials regularly. The reason why there could be failures in these could be attributed to whatever is going on inside the mind of the person maintaining the systems, such as mental burnout, stress, or fatigue. Factors such as these could cause someone to not be as careful or as willing to work up-to-standard for maintaining systems regularly and being diligent in their work. With these factors in mind, people can also become more susceptible to social engineering attacks if they were to fall victim to such attacks. Phishing, for example, can become easier to fall for if someone is stressed or is feeling tired, as these emotions can influence and cloud our judgment to then choosing what the right choice is much more challenging to do compared to when mental factors are not in-play. Therefore, one should be careful in ensuring that their mental well-being does not dampen their line of work in ensuring proper cybersecurity for themselves and organizations as a whole.

Two examples of cybersecurity risks and vulnerabilities that are related to human actions include falling for social engineering tactics and having poor password security, contributing greatly to cybersecurity incidents and vulnerabilities. A social engineering tactic, for example, can include phishing, which is a type of cyberattack that manipulates the victim to disclose confidential information, such as a password, to the hacker. These types of attacks can appear as an email, for example, let's say "Microsoft" sent an email saying that I need to change my password or I need to tell them my password in order to be secured from future data breaches. Some individuals may take the email as legitimate, and not think about the possibility that the real sender may not be Microsoft, but rather, someone else who manipulates victims in order to get the information that they want. Poor password hygiene is also another good example of how human behavior can contribute to cybersecurity incidents and create vulnerabilities. This type of human behavior can include using the same passwords across multiple work platforms, or using weak passwords that are easy for people to guess. Many individuals often do this human behavior because they don't want to memorize a long, complicated password or rather multiple complex passwords for multiple different sites, so they choose to both use the same password for every site that they have an account in and keep the password short and simple so it is easy to remember. Both of these human behaviors of falling for social engineering tactics and poor password hygiene can easily be solved by educating individuals and organizations about social engineering tactics and how to identify them, and also the importance of using a different, strong password for each site to ensure good password hygiene

Social factors also play a role in decision-making. This can include down-playing vulnerabilities, such as being influenced by colleagues who follow what each other does rather than following organization policy. Another factor can include groupthink, which is the idea that

everyone downplays severe cybersecurity risks because everyone believes that a system is secure, even when it truly isn't. This becomes especially dangerous because some may identify and recognize severe risks, but not say anything about the risks because they don't want to annoy their other colleagues or create a lot of work to figure out remedies to address the risks. Therefore, it should be important for organizations to emphasize the following phrase: if you see something that's wrong, speak up. There is nothing wrong with reporting a problem, in fact it's the correct thing to do. By emphasizing this phrase and ensuring everyone is following organization policy rather than the policy of each other, organizations can potentially help mitigate certain social factors that could impact cybersecurity and make it more vulnerable.

Organizations can however reduce the number of incidents and vulnerabilities associated with the human factor in cybersecurity by training employees and ensuring the overall wellbeing of employees. This training can include educating employees about risky cybersecurity behaviors and warning signs to look for to identify a social engineering attack. In the real world, for example, companies could also run phishing simulations to test their employees to measure if their employees have learned anything from their training. It is worth noting that these simulations are most often unannounced to properly observe the true actions and decision-making of the employee. According to Truleap Technologies, a telecommunication and managed information technology provider based in southern Idaho, they say "Unannounced phishing simulations are effective in evaluating employees based on how much they have learned. It would surprise you how so many people do well in theory but still won't be able to tell the real deal when it is staring at them from the inbox. Being bitten once in a simulated attack will teach your employees to be more vigilant" (Truleap Technologies, n.d.). By training employees on a regular basis in simulations such as these, organizations can ensure that their

employees are less at risk of falling victim to social engineering attacks. Additionally, organizations should also ensure the overall wellbeing of their employees so that they will be less susceptible to making mistakes that negatively impacts cybersecurity. This can include making sure that employees are not being overworked, and also performing a wellness check on every employee in some capacity to observe if certain emotions could be affecting the overall diligence of their work.

The human factor plays a significant role in the field of cybersecurity, with social factors and behaviors coming together to influence the overall effectiveness of cybersecurity. This paper serves to explain how social factors and behaviors influence cybersecurity vulnerabilities and risks, and how organizations and individuals alike can help promote positive behaviors and actions. When organizations and individuals promote positive behaviors and actions, cybersecurity itself is strengthened and the risk of bad behaviors and actions occurring is greatly reduced, which overall reduces the number of potential cyber breaches to occur because of human behaviors and actions.

References

Truleap Technologies. (n.d.). *Training employees to spot social engineering*. https://truleap.net/training-employees-to-spot-social-engineering-filer-id/