The Impact of Human Error on Organizational Security and Its Mitigation Through Training and Awareness Programs

Gregory S. Oehm

School of Cybersecurity, Old Dominion University

CYSE 495: Human Factors and Policy in Cybersecurity

Prof. Saltuk Karahan

August 3, 2025

Introduction

The human factor is quite important for organizational leaders and cybersecurity professionals to consider in the creation of the cybersecurity policies and plans used within their organization. Certain perspectives employees might hold in relation to cybersecurity can contribute to significant vulnerabilities, which have the potential to be exploited by attackers, should the proper steps not be taken to alter them. There are, however, major steps that can be taken to mitigate the impact that human error can have on organizational security. One of the most helpful of these methods is the implementation of a cybersecurity training and awareness program, which can help foster support for more secure behaviors, educate users on new and rising threats, and work to create a culture that works in tandem with the organization's cybersecurity goals, rather than against them.

The Importance of the Human Factor in Cybersecurity Outcomes

The human factor is one of the most important considerations organizational leaders must address in the cybersecurity posture of their organization. Reducing human error is critical to the security of organizations, with a significant majority of successful attacks being caused or permitted by human error, rather than through a failure of technical controls or other hardware and software vulnerabilities (Kenlie et al., 2024). Social engineering is one of the most important ways in which human error is leveraged by attackers to gain access to an organization’s systems and information. The 2014 breach of Sony Pictures is one notable example of a social engineering attack being successfully executed. In that incident, it is thought that North Korean attackers utilized targeted spear-phishing emails to gain access to employee login credentials, and thus their company’s infrastructure (*North Korean Programmer Charged*, 2018). At that point, the attackers exfiltrated significant amounts of sensitive data that was later released

publicly (*North Korean Programmer Charged*, 2018). Phishing, and its more targeted version spear-phishing, utilize emails aimed at tricking individuals into giving up sensitive information, such as passwords. These emails often include a sense of urgency in order to encourage swift action, and may possess the branding of an otherwise reputable company, in order to inspire trust. Though phishing is perhaps the most prevalent form of social engineering, many other types do exist, including tailgating, baiting, and pretexting, among countless others. Through these attacks, the trust and inconsistency that humans bring to an organization can be taken advantage of. Any one person out of potentially thousands, through a simple mistake, can end up enabling a breach or other attack to occur against the organization, along with the massive damage they can cause. The average breach might cost organizations several million dollars, taking into account the many indirect effects of the attack (Thakur et al., 2024). This demonstrates the damage that unfamiliarity or carelessness with cyber threats can cause within an organization. It is worth noting, however, that while there may be significant reason to fault these individuals for their actions, punishment alone might not be able to resolve the underlying issues that enabled this behavior. This potentially prevents effective actions from being taken to mitigate the issue in the future, through reducing trust, where a lack of effective training and awareness built into the organization, that could have prevented these attacks, may be to blame. Employees within an organization may not follow the proper procedures because they believe that security goes against their objectives, they are unaware of or apathetic to the need for security in its entirety, or they are simply not trained to engage in more secure behaviors, among other reasons, meaning that humans are almost always the weakest point in the security of essentially any organization. This, of course, goes beyond both technical measures and the

distribution of basic information surrounding policies and technical factors. Another, more social method is thus necessary to combat human error and the harm it might cause to organizations.

Mitigating Human Error Through Training and Awareness

Cybersecurity training and awareness programs are crucial to mitigate the negative impacts this kind of human error can have on the overall security posture of the organization. Cybersecurity professionals, alone, cannot combat these sorts of threats, as they have little direct control over how users go about their duties. Given that this is largely a human problem, by its very nature, it requires a solution that takes into account the behavior and attitudes of these people. Encouraging compliance with organizational policies and implementing other non-technical solutions are, thus, clearly needed to address this issue in the perspectives and mindsets of employees. Awareness of the specific actions encouraged and restricted within these documents is necessary to prompt compliance with them. It is worth noting that the knowledge of organizational policies and the appropriate behaviors they delineate, by itself, does not necessarily lead to changes in behavior. Awareness alone, while perhaps prompting brief improvements in behavior, is not likely to prompt the long-term changes in culture, perspectives, and behavior that organizations need to stay secure (Alshaikh & Adamson, 2021). By implementing strong training and awareness programs within the organization, however, its creators can work to influence the opinions and habits of individuals, thereby fostering support for the actions that work in favor of the organization's overall goals, both in its security and its general functioning. These cybersecurity training and awareness campaigns will likely only be effective if they are carried out in the appropriate manner. Several techniques exist to bolster the effectiveness of these campaigns, enabling them to prompt real, discernable change in the behaviors of individuals, rather than simply being token nods to the importance of security, the

memory of which being quickly discarded from the minds of users. Perhaps the most important factor contributing to the success of these programs is their ability to get employees or other users to engage with and relate to the topics discussed. Users may be unwilling to alter their routine if the reasoning behind secure behaviors seems disconnected from their day-to-day activities. Relating information about cybersecurity to each user, such as by connecting it to whichever specific job they perform, can allow this information to be more memorable, more engaging, and thus more likely to be actually applied in practice. Several other methods exist to promote engagement with cybersecurity education, as well. Presentations that inspire real conversations among listeners, for instance, rather than those that simply relay information, can encourage greater participation with the content. Gamification, or using games to help train users, can also be effective in this regard, though the quality of the game might play a large role in this (Hussein Sharif & Yousif Ameen, 2021). Training should also be consistent and regular, as opposed to spontaneous and infrequent. It is crucial that this is routinely carried out, so as to not have employees begin to rest on their laurels. Emails can help accomplish this, communicating important points daily or weekly while simultaneously enabling communication with all people in the organization, rather than a subset of specific individuals. Phishing tests, or activities that simulate other forms of social engineering can also be performed routinely, with the added benefit of highlighting to individuals that threats are real, not hypothetical. The tangibility of these kinds of tests provide can demonstrate to employees or other users that they, themselves, are susceptible to certain attempts made by attackers to gain access to organizational resources, and will consequently be more likely to truly listen and internalize the information provided through both this method and others. Posters or other physical media can serve as consistent reminders of important considerations in regards to cybersecurity and organizational

policy, as well. Physical reminders, such as these, are a way to disseminate knowledge relatively unintrusively, and with little effort. Each of these approaches extends the training and awareness provided by the training and awareness program far beyond any specific event, into a continuous effort that is regularly seen by each user. Not only does this permit users to be kept abreast of recent changes in the threat landscape that might impact certain departments or the organization as a whole, it also allows the overall motivations behind secure behaviors and perspectives to be fresh in the minds of users, with the most important lessons not being forgotten over time. No matter which specific methods are employed, or the exact information discussed within these methods, organizations are likely to see at least some improvements in the secure behaviors of users (Prümmer et al., 2024). Altogether, it is necessary to engage in training and awareness programs that take into account the needs and mindsets of employees or users. While the exact implementation of a training and awareness programs should be based on the needs of the organization and the context it finds itself it, a program that encourages secure behaviors and builds a culture within the organization and favors cybersecurity as a worthwhile goal in and of itself, rather than an obstacle that needs to be dealt with by users, will be far more successful than those that focus on knowledge alone.

Conclusion

The human factor, in addition to technical vulnerabilities, are both necessary to consider in order to mitigate all forms of vulnerabilities that might be present within an organization. Social engineering seeks to exploit the trust of humans, rather than any kind of technical fault that might be present in certain systems, and is thus especially dangerous. Training and awareness programs can help to shore up the vulnerabilities brought into the organization by humans, but these have to be done correctly in order to gain the most advantages possible. Such

campaigns should be engaging, rather than tedious. Otherwise, they may be seen as just another obstacle in the name of cybersecurity. If implemented well, cybersecurity training and awareness campaigns should bring about positive attitudes towards cybersecurity, and can inspire employees within the organization to enthusiastically support cybersecurity and the many benefits it can provide.

References

Alshaikh, M., & Adamson, B. (2021). From awareness to influence: toward a model for improving employees' security behaviour. *Personal and Ubiquitous Computing*, 25, 829–841. https://doi.org/10.1007/s00779-021-01551-2

Hussein Sharif, K., & Yousif Ameen, S. (2021). A review on gamification for information security training. *2021 International Conference of Modern Trends in Information and Communication Technology Industry*. https://doi.org/10.1109/MTICTI53925.2021.9664771

Kenlie, E. A., Hendris, C. N., Nadia, N., & Adeta, F. (2024). The impact of human error in Cybersecurity breaches: Understanding behavioral patterns and mitigation strategies. *2024 International Conference on Informatics, Multimedia, Cyber and Information System*, 1045–1050. https://doi.org/10.1109/icimcis63449.2024.10956680

North Korean programmer charged in Sony hack, WannaCry attack. (2018, September 6). PBS News. Retrieved August 3, 2025, from https://www.pbs.org/newshour/nation/north-korean-programmer-charged-in-sony-hack-wannacry-attack

Prümmer, J., Van Steen, T., & Van Den Berg, B. (2024). A systematic review of current cybersecurity training methods. *Computers & Security*, 136. https://doi.org/10.1016/j.cose.2023.103585

Thakur, K., Barker, H., & Ali, M. L. (2024). Human error in cybersecurity management. *2024 IEEE Technology and Engineering Management Society*. https://doi.org/10.1109/temsconlatam61834.2024.10717786