CSA Training vs Cybersecurity Technology in Dealing with the Human Factor

In an organization, a Chief Information Security Officer would have to consider the human factor, and the risk people cause to cybersecurity during the creation and implementation of their security policies. This would include, determining how to spend the funds the company has available for IT security. Part of this decision process involves deciding the importance of cybersecurity awareness (CSA) programs vs cybersecurity technology. CSA training helps to educate employees on common cybersecurity threats and scam tactics, and cybersecurity technology works to prevent and expose security threats before and as they arise so that a cybersecurity professional can work to eliminate the threat. While cybersecurity awareness training is incredibly important and can help to prevent some common human error threats, human error will always be a factor which is why there should be a healthy balance between cybersecurity technology and CSA training.

The Human Factor in Cybersecurity:

Human factor relates to cybersecurity in a few main ways. The first, is how technology should be developed with how the human brain works in mind. This means taking into account how people will intuitively try to work with the technology during the development process. Secondly, and perhaps the more often discussed aspect of the human factor in cybersecurity, is the risk that humans pose to IT security. People are one of if not the greatest threat in cybersecurity, and the human factor is often related to human error (Learning Center, 2024).

Cybersecurity Awareness Training:

Cybersecurity awareness programs are courses that help to teach people about cybersecurity. These typically cover common scamming tactics and how to identify them, how to adhere to security policy requirements, strong password management, internet safety, and more general cybersecurity knowledge (Kaspersky, 2025). These training programs are so important because of the amount of cybersecurity issues caused by people simply not knowing cyber safety. Hackers will often take advantage of that lack of knowledge in order to do damage to either the individual or their organization or possibly even both. Organizations use these programs to help inform their employees in order to protect the company's data.

Cybersecurity Technology:

On the other hand, cybersecurity technology is the software and hardware designed to protect systems from malicious attacks. Some benefits of technical security are that it doesn't require outside input to deal with security threats as they happen and they are always working (Pierson Tech Blog, 2024). Security technology helps to catch attacks that humans may miss. Even though no security system is without its faults, it is much more likely to prevent an attack than just people alone. Cybersecurity systems also help to identify and block, more types of attacks than just those that may be caused by social engineering.

Where Limited Funds Would Be Allocated:

Ideally, an organization would be able to thoroughly fun both cybersecurity awareness programs as well as cybersecurity technology. Unfortunately, this may not be a possibility for many companies and organizations, especially if they are on the smaller side. These elements of security work really well together because they can help to catch threats that the other may miss.

If possible, funds should be balanced pretty equally between the two. However, if one must be picked over the other, the focus should be on technical security because even with security training there will always be human errors. Although security technology is also not fool proof and can make its own mistakes, it is much less likely.

Conclusion:

The human factor is one of the main considerations in cybersecurity development. Chief Information Security Officers often have to decide whether to focus their funding on CSA training or technical security by taking into account the risks associated with the human factor. Both are incredibly important to the defenses of an organization's cybersecurity. Cybersecurity awareness training helps to educate the people and fortifying the technical security aspects helps to catch any threats people may miss. If only one can be reinforced within a company, it should be the cybersecurity systems in order to maximize the protection from cyber-attacks.

Works Cited:

Kaspersky. (2025). *A Comprehensive Guide to Cybersecurity Training*. Retrieved from Kaspersky: https://usa.kaspersky.com/resource-center/preemptive-safety/cybersecurity-training

Kaspersky. (n.d.). *The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within*. Retrieved from Kaspersky Daily: https://www.kaspersky.com/blog/the-human-factor-in-it-security/

Learning Center. (2024, February 16). *The Human Factor in Cybersecurity*. Retrieved from Security Scorecard: https://securityscorecard.com/blog/the-human-factor-in-cybersecurity/

Pierson Tech Blog. (2024, November 25). *Security Awareness Training vs. Technical Controls*. Retrieved from Pierson Tech: https://pierson-tech.com/blog/f/security-awareness-training-vs-technical-controls?blogcategory=Comparing