Daija Brown

Mr. Kirkpatrick

Cybersecurity, Technology & Society-200T

3/16/2026

Managing the Human Factors of Cybersecurity as a CISO

To mitigate the vulnerabilities associated with humans in cybersecurity, a system must be created with humans in mind. This requires implementing strong administrative controls, providing incentives for employee participation, and threat detection and prevention tools.

Administrative Controls

Educating the organization is the primary goal to mitigate the risks associated with human factors. “In fact, more than two-thirds of successful cyberattacks involve human error in the targeted company” (Anderson). Mandatory annual cyber security awareness training can be effective if it has a knowledge check built in that requires the user to answer questions correctly to pass the training. Phishing simulations could be used to gauge an organization’s competency with identifying and reporting phishing emails. The metrics from the annual training and phishing simulations could identify weak points in my training program. I could use that information to advise what revisions need to be made.

Policies such as the Acceptable use and Enterprise Risk Management policy will be mandatory. This establishes what is considered appropriate behavior for the network and on company assets. Because these policies are mandatory, it makes everyone

accountable for their behavior. Violations of these policies could lead to a write up and repeat offenses could lead to termination of employment. Another administrative control I would implement is the principle of least privilege. This will mitigate risks associated with lateral movements and unauthorized access.

Technology

The physical and logical assets will be used to mitigate the residual risks after the training program is established. The primary responsibility of these assets is to establish a baseline for the network so it can detect, report, and block anomalies. To obtain this baseline, I would recommend a firewall. Firewalls operate 24/7 and can be configured to enforce written policies. For example, if the policy prohibits downloading software without permission, the firewall could be configured to block software downloads. If a user needs to download software, they could submit an exception request.

A Security Information and Event Management (SIEM) tool should be paired with the firewall to provide advanced threat detection. “SIEM increases efficiency by filtering unnecessary data and only showing you what you need to see. It cuts through the noise to help your team create an informed security strategy and response plan” (Singh). While a SIEM may seem expensive, it is a proactive tool that may identify threats based on configurations. This pairs well with the firewall because the firewall is focused on blocking threats.

Incentives

Rewarding users for “doing the right thing” encourages the culture of security, which reduces risky behaviors. “If you never reward employees for engaging in good cyber behavior and only provide consequences for risky cyber behavior, employees will associate cybersecurity only with consequences and it will have a negative connotation for them” (Beauceron Security). While prizes may be used to reward good behavior, the rewards do not have to be monetary. For example, a “phishing license” could be rewarded to users who have reported simulated phishing attempts. If a user obtains a predetermined amount of phishing licenses, their reward could be a week of parking in the CISO’s designated parking spot, or one free day of PTO.

Conclusion

In conclusion, education, technology, and incentives are important components to mitigate the risks associated with the human factor of cybersecurity. Another thing to consider is the influence of leadership on individual contributors. Trust in leadership is a contributing factor for mitigating risky behaviors in compliance. This means the behaviors we want to see throughout the organization must start at the top and trickle down.

Works Cited

Anderson, Elliot. “Why User Education is #1 in Cyber Resilience.” *lumifi*, 19 December 2020, https://www.lumificyber.com/blog/why-user-education-is-important-cybersecurity-resilience/. Accessed 22 March 2026.

Beauceron Security. “How to Implement Consequences and Rewards in Your Security Awareness Program.” *Beauceron Security*, No date, https://www.beauceronsecurity.com/blog-english/how-to-implement-consequences-and-rewards-in-your-security-awareness-program. Accessed 22 March 2026.

Singh, Navcharan. “SIEM vs. Firewall.” *PeerSpot*, 7 October 2022, https://www.peerspot.com/articles/siem-vs-firewall. Accessed 22 March 2026.