The Human Factor in Cybersecurity

Shayla Harmon

Old Dominion University

CYSE 200T

Charlie Kirkpatrick

September 27, 2026

The Human Factor in Cybersecurity

The human factor is an important part of cybersecurity because people's decisions and behaviors can either protect an organization or create security vulnerabilities. Actions such as clicking phishing links, using weak passwords, or accidentally sharing sensitive information can give cybercriminals opportunities to access systems and data. Organizations can reduce these risks through regular training, clear security policies, communication, and a workplace culture where employees understand their responsibility for cybersecurity.

What is the Human Factor in Cybersecurity?

The human factor in cybersecurity refers to the way people's actions, decisions, behaviors, and mistakes can affect the security of computer systems and information. Cybersecurity is often associated with technology such as firewalls, encryption, and access controls. However, technology is only one part of protecting an organization. The people who use these systems also play an important role in keeping them secure. Even if an organization has strong technical controls, human behavior can still create vulnerabilities that attackers can use.

Phishing and Social Engineering

One major cybersecurity risk related to human behavior is phishing. Phishing is a type of social engineering attack in which an attacker attempts to trick someone into providing sensitive information by clicking on a malicious link. Aldabagh et al. (2025) states that phishing continues to be a major threat because it is simple and effective. In addition, attackers may create emails or messages that look legitimate and will use familiar company names, logos, or urgent requests.

For example, an employee may receive an email stating that their account will be locked unless they click a link and sign in. If the employee does not recognize the warning signs, they could provide their username and password to a threat actor. The attacker could then use that

information to access company systems or sensitive information. Aldabagh et al. (2025) also states once the attacker is granted access to the information, it often leads to financial harm and misuse of personal information. Phishing is effective because it takes advantage of human emotions such as fear, urgency, curiosity, and trust.

Weak Passwords and Poor Security Practices

Another cybersecurity risk is weak password practices. Employees may create passwords that are easy to remember but also easy for attackers to guess. Some people may also reuse the same password for multiple accounts. Aldabagh et al. (2025) states, if one account is compromised, an attacker may try the same username and password on other systems. This can increase the damage caused by a single security incident.

Companies can reduce this risk by requiring strong passwords and using muti-factor authentication (MFA). MFA provides an additional layer of security because a password alone is not enough to access an account. Organizations should implement frequent trainings for employees about the importance of protecting their passwords and avoiding password reuse.

Reducing Human Related Cybersecurity Risks

Organizations can reduce human related cybersecurity risks through training, clear policies, communication, and a strong security culture. Cybersecurity training should not only be something that employees complete once a year. Organizations should provide regular training that teaches employees how to recognize phishing attempts, create secure passwords, protect sensitive information, and report suspicious activity. Simulated phishing exercises can also help employees recognize common attack techniques in a safe environment.

Clear policies are important because employees need to understand what is expected of them. Policies should explain appropriate password use, access to company systems, how

sensitive information should be handled, and how security incidents should be reported. Companies should also implement security strategies and steps like, collect and analyze, detect, deter, protect, predict, and react (Aldabagh et al., 2025, p. 95). Furthermore, employers should feel comfortable reporting mistakes because if they are afraid of being punished, they may avoid reporting them which can become a larger security concern.

Psychological, Social, and Organizational Factors

Psychological, social, and organizational factors can influence how people make cybersecurity decisions. People are more likely to make mistakes when they are stressed, distracted, rushed, or overwhelmed with work. For example, an employee may be more likely to respond to an urgent request if they believe it came from a supervisor or coworker. Attackers can take advantage of these behaviors when using social engineering techniques.

Organizations should recognize that employees are human and will sometimes make mistakes. Creating a workplace culture where employees are encouraged to ask questions and report suspicious activity can help improve security. Employees are more likely to follow security practices when they understand why those practices are important rather than simply being told what rules to follow.

Conclusion

The human factor is an important part of cybersecurity because people can either strengthen or weaken an organization's security. Phishing, weak passwords, and poor security practices can create opportunities for cybercriminals. Organizations cannot eliminate human error, but they can reduce the risk by providing effective training, creating clear policies, limiting access, applying muti-factor authentication, and building a positive security culture. To conclude, protecting an organization requires more than just having the right technology in place

because employees need to understand how to make good decisions when using technology and handling information.

References

Oesteraas, I. L. (2025). Criminal justice and cybersecurity. In H. Aldabagh, C. Bowman, I. Kirkpatrick, I. L. Oesteraas, & V. L. D. Yalpi (Eds.), *Cybersecurity, technology & society* (pp. 69–140). Old Dominion University.