Sergio Hunter

Professor Kirkpatrick

CYSE200T_14936

28 September 2026

The Risks Created from Human Behavior in Cybersecurity

Human behavior in cybersecurity poses a major vulnerability that malicious individuals can take advantage of to attack or gain unauthorized access to organization's information systems and equipment. While human behavior will always be present and exploited within organizations through means like social engineering and poor password management, organizations can reduce these risks by implementing strong workplace policies, proper training, and communicating effectively.

What the "Human Factor" is in Cybersecurity

The human factor in cybersecurity refers to "how human behavior, decisions, actions, and mistakes influence an organization's security posture. While cybersecurity technologies continue to advance, people remain one of the most significant sources of cyber risk (Sepio, 2025)." It is a known fact that people are considered the most frequently targeted vector in cybersecurity incidents, but how exactly does human behavior contribute to cybersecurity incidents? There are a few contributing factors: people are prone to making mistakes while performing routine operations in their occupations; humans are guided by emotions and morals that may make them susceptible to manipulation by attackers; employees may not be properly trained to handle situations involving potential cybersecurity threats; and employees could potentially use their privilege to deliberately attack the organization from within. A good example of improper

training would be an organization failing to teach employees how to report a potential phishing email to the IT department. This could prevent the IT team from reviewing potential malicious content and notifying users across the organization of it.

Identifying Cybersecurity Risks Related to Human Actions

There are many actions that malicious individuals can take to attempt exploiting human behavior within an organization. One of those ways is social engineering. Social engineering attacks occur "when hackers try to trick employees into exposing sensitive internal information, either via a phone, in-person conversation, or an internal messaging tool, such as Slack (Kost, 2026)." These hackers can potentially trick employees into giving up sensitive information by posing as a higher-up within the company, using personal information to blackmail them, or making them react quickly by making a message seem urgent. A good example would be an attacker posing as the CEO of a company and sending an email to the finance department requesting the most recent financial audit report. Another way malicious individuals may gain unauthorized access to sensitive organizational information is through poor password management. Poor password management by an organization can include practices like keeping factory-set passwords for accounts and equipment, not requiring multi-factor authentication methods for login verification, reusing the same password for multiple systems and websites, and saving passwords through insecure means, such as writing it on a sticky note and leaving it out on an office desk.

Strategies Organizations Can Use to Reduce Human-Related Risk

While organizations may not be able to prevent all cybersecurity risks associated with human behavior, there are ways these risks can be reduced. A good place to start is implementing strong password policies. Organizations should require multi-factor authentication for all users to add an extra security layer when accessing accounts or systems. Establishing policies that require strong, complex password and frequent password changes will also provide effective protection against potential attackers. Next would be to provide employees with proper training for detecting malicious attempts to gain unauthorized access to systems and sensitive information. Something like phishing simulations would help employees see what real world phishing attempts look like and how they can report them to the IT team. This leads to effective communication. When employees can demonstrate adequate communication across departments regarding cybersecurity risk, organizations can identify potential threats quickly and respond accordingly to the risk to reduce the impact they may have.

Conclusion

Cybersecurity risks associated with human behavior are a continuous battle that organizations will have to pay close attention to in order to mitigate and prevent any looming threats. While there are best practices organizations can implement in their environment, it's important to take into consideration why people may make a certain cybersecurity decision as well. There are psychological factors like overconfidence that cause employees to be less careful when approaching potential threats. There are also social factors like office norms that could encourage employees to not take policies seriously if they see others across the organization

neglecting policies. By understanding these factors, organizations can work to develop adequate strategies for reducing human-related cybersecurity risks and strengthen their overall security.

References

Sepio (2025, May 22). *Human Factors in Cybersecurity: Reducing Human Cyber Risk*. SepioCyber. Retrieved on September 28, 2026. https://sepiocyber.com/blog/human-factors-in-cybersecurity/

Kost, E. (2026, July 2). *Human Factors in Cybersecurity in 2026.* Upguard. Retrieved on September 28, 2026. https://www.upguard.com/blog/human-factors-in-cybersecurity

Myers, A. (2026, February 9). *Weak Passwords & Password Policies: Strengthening Access Security*. Cyberlab. Retrieved on September 28, 2026. https://cyberlab.co.uk/blog/weak-passwords-and-password-policies/