The Human Factor in Cybersecurity

Marion Watkins

Old Dominion University

September 28, 2026

The Human Factor in Cybersecurity

When people think about cybersecurity, they usually think about computers, firewalls, passwords, or some hacker sitting behind a screen. Those things are important, but the human side of cybersecurity is just as important. The "human factor" is basically the way people's choices, mistakes, habits, and reactions can affect the security of an organization. A company can have expensive security tools and still have problems if an employee clicks a bad link, gives away a password, or ignores a security rule. Verizon's 2025 Data Breach Investigations Report found that the human element was involved in about 60% of confirmed breaches, which shows that cybersecurity is not only a technology problem (Verizon, 2025).

How Human Behavior Creates Cybersecurity Risks

Human behavior can create cybersecurity vulnerabilities in ways that are sometimes very simple. People get busy, distracted, curious, or pressured, and attackers know that. Cybercriminals do not always need to break through a complicated technical defense if they can convince someone to open the door for them. This is one reason social engineering is such a big issue in cybersecurity.

One common example is phishing. A phishing email may look like it came from a bank, a manager, a school, or another trusted organization. The message might tell the person that they need to click a link immediately, reset a password, or confirm some information. If the person

does not slow down and check the message, they could give an attacker their login information or download malware. CISA explains that phishing often tries to get people to open harmful attachments or give up personal information (Cybersecurity and Infrastructure Security Agency [CISA], n.d.). The scary part is that the technology does not have to be defeated. The attacker is trying to defeat the person instead.

Weak or reused passwords are another example. Someone might use the same password for multiple accounts because remembering a bunch of different passwords is annoying. If one website is breached, an attacker could try that same password somewhere else. This turns one small mistake into a much bigger problem. Strong passwords, password managers, and multifactor authentication can reduce this risk (CISA, n.d.).

Why People Make These Mistakes

It is easy to say that someone should just "be more careful" but that does not really explain why these mistakes happen. People make cybersecurity decisions based on the situation they are in. For example, an employee who is rushing to finish something might click an email without checking it closely. Someone who receives a message that appears to come from their boss may feel pressure to respond quickly. Attackers can take advantage of urgency, authority, fear, curiosity, and trust.

Workplace culture also matters. If employees are afraid of getting in trouble for reporting that they clicked something suspicious, they might hide the mistake instead of telling the security team. That can make the incident worse. On the other hand, if an organization treats reporting as part of the job instead of immediately blaming people, employees may be more willing to speak up. Verizon has also pointed to increased reporting of phishing attempts as an important part of building a stronger security culture (Verizon, 2024.

This is why cybersecurity cannot be treated as only an IT department's responsibility. Employees in different jobs interact with systems and information every day. A person in accounting, human resources, management, or customer service can make a decision that affects the organization's security just as much as someone working directly in IT.

Reducing Human-Related Cybersecurity Risks

Organizations can reduce these risks by combining technology with training, clear policies, and a good workplace culture. Training should not just be a boring presentation that employees complete once a year and immediately forget. It should use realistic examples and explain what employees should actually do when they see something suspicious. NIST recommends an ongoing cybersecurity and privacy learning program that focuses on awareness, education, behavior change, and improvement over time (Merritt et al., 2024).

Organizations can also use technical controls to give people another layer of protection. Multifactor authentication can make a stolen password less useful. Email filtering can block some malicious messages before employees see them. Password managers can help people avoid reusing passwords. These tools do not replace good decisions, but they can limit the damage when someone makes a mistake.

Policies also need to be realistic. If a security policy is so complicated that employees cannot follow it during a normal workday, people may start ignoring it. Managers have to follow the same rules as everyone else too. It would be hard to convince employees that cybersecurity matters if management constantly skips security procedures whenever they are inconvenient.

Conclusion

The human factor is one of the biggest parts of cybersecurity because technology is still being used by people. Phishing, weak passwords, social engineering, and workplace mistakes

can all create opportunities for attackers. At the same time, blaming employees for every incident does not solve the problem. Organizations need to make secure behavior easier, provide useful training, encourage people to report mistakes, and use technical protections as another layer of defense. Cybersecurity works better when people understand that they are part of the security system instead of thinking security is only the IT department's job. At the end of the day, even the best security system in the world can have a bad day if someone clicks the wrong button.

References

Cybersecurity and Infrastructure Security Agency. (n.d.). Secure our world. U.S. Department of Homeland Security. https://www.cisa.gov/secure-our-world

Merritt, M., Hansche, S., Ellis, B., Nethery Snyder, J., Sanchez-Cherry, K., & Walden, D. (2024). Building a cybersecurity and privacy learning program (NIST Special Publication 800-50 Rev. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-50r1

Verizon. (2024). 2024 data breach investigations report. Verizon Business. https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf

Verizon. (2025). 2025 data breach investigations report. Verizon Business. https://www.verizon.com/business/resources/reports/2025-dbir-data-breach-investigations-report.pdf