waystone | Compliance Solutions

The Human Factor in Cyber Security: Understanding the Impact of Human Error

John Zuska February 25, 2025

When discussing cyber security, many focus on firewalls, encryption and cutting-edge technologies. However, the greatest vulnerability in most organizations isn't a piece of software or hardware; it's human error.

In fact, research shows that human mistakes are responsible for most cyber security breaches. Whether it's falling for phishing emails, mismanaging passwords, or mishandling sensitive data, employees can unintentionally expose organizations to significant risks.

For February, we'll explore the role of human error in cyberattacks, common mistakes employees make, and how businesses can implement effective training and awareness programs to mitigate these risks.

The Role of Human Error in Cyberattacks

Cybercriminals know that humans are the weakest link in any security system. Social engineering tactics, such as phishing and pretexting, prey on human psychology. For instance, employees may be tricked into clicking malicious links, providing sensitive credentials, or even wiring money to fraudulent accounts.

Some of the most infamous cyberattacks have been enabled by human error. The 2017 Equifax breach, which exposed the personal data of 147 million people, stemmed from a failure to apply a software patch. Similarly, the 2020 Twitter hack involved employees being duped through a phone spear-phishing attack.

Common Mistakes Employees Make

Let's take a closer look at some of the most frequent errors that can lead to cyber security incidents:

Falling for Phishing Scams

Employees often fail to recognize phishing emails or messages. These scams use legitimate-looking content to deceive users into providing sensitive information or downloading malware.

Weak or Reused Passwords

Using simple or repeated passwords across accounts makes it easier for attackers to gain access. Despite widespread awareness, password mismanagement remains a top issue.

Unintentional Data Exposure

Sharing sensitive information over unsecured platforms, emailing confidential files to the wrong recipient, or failing to encrypt critical documents are all forms of accidental exposure.

Neglecting Security Updates

Delaying or ignoring software updates and patches leaves systems vulnerable to known exploits.

Improper Use of Devices

Using personal devices for work without adequate security measures, or vice versa, can open gateways for attackers. In the same way, lost or stolen devices without encryption can compromise data security.

Prevention Strategies: Building a Human Firewall

Organizations must acknowledge the role of human error and take proactive steps to address it. Here are effective strategies firms can implement:

Comprehensive Training and Awareness Programs

- Regularly train employees on identifying phishing attempts, safe browsing habits, and secure password practices.
- Conduct phishing simulations and other interactive exercises to help employees recognize and respond to threats.
- Customize training materials to suit different roles within the organization. For example, finance teams might receive additional guidance on spotting invoice fraud.

Establishing Clear Policies and Guidelines

- Develop clear cyber security policies that outline acceptable use of devices, secure communication channels, and incident reporting procedures.
- Create guidelines for remote work environments to ensure employees follow security protocols when working outside the office.

Promoting a Culture of Cyber Security

- Encourage employees to adopt a security-first mindset. Reward positive behaviors and foster an environment where individuals feel comfortable reporting potential security risks without fear of blame.

Leveraging Technology to Minimize Risks

- Use multi-factor authentication ("MFA") to add an extra layer of protection to accounts.
- Implement endpoint protection and monitoring tools to detect unusual activity.
- Deploy automated tools for patch management to ensure systems remain updated.

Conducting Regular Risk Assessments

- Continuously evaluate the organization's risk landscape. Identify areas where employees may require additional support or resources.
- Use penetration testing to simulate real-world attacks and identify vulnerabilities in employee practices.

Final Takeaways: Strengthening Cyber Security Through People

While technology plays a vital role in safeguarding digital assets, the human element cannot be overlooked. By addressing common mistakes and equipping employees with the knowledge and tools to recognize threats, organizations can transform their workforce into a robust line of defense against cyberattacks.

Cybersecurity is everyone's responsibility. By investing in awareness and fostering a culture of vigilance, businesses can significantly reduce the risks posed by human error and create a safer digital environment in 2025 and beyond.

How can Waystone help?

Waystone Compliance Solutions is a leading provider of cyber security consulting and compliance services to the financial services industry. If you would like to find out how Waystone can help you to assess your current cyber security measures, please reach out to your usual Waystone representative, or contact us below.

Contact Us →