Charles Kraiger Explains Why Employee Training and Awareness Are the First Line of Defense In Cybersecurity

Charles Kraiger Explains Why Employee Training and Awareness Are the First Line of Defense In Cybersecurity

Los Angeles, California Sep 24, 2025 (Issuewire.com) - Data breaches continue to dominate headlines, but cybersecurity analyst Charles Kraiger says most can be prevented with better employee awareness. Charles Kraiger, a seasoned cybersecurity expert with over a decade of experience analysing threats and strengthening defences, calls on businesses to prioritize training as the most effective tool in reducing cyber risk.

“Technology alone cannot protect organizations from cyberattacks,” says Kraiger. “The truth is, most breaches start with human error. Phishing emails, weak passwords, or the accidental download of malicious files are often the open doors that attackers exploit. Closing those doors requires well-trained employees who can spot threats before they spread.”

The Human Element: A Persistent Vulnerability

While companies invest heavily in firewalls, encryption, and intrusion detection systems, the majority of data breaches are caused by human mistakes. Studies have shown that nearly 90% of cyber incidents involve some element of human error. A single careless click or a reused password can undermine millions of dollars of security investment.

Charles Kraiger emphasizes that employees should not be viewed as weak points but as critical allies. “When you build a culture of awareness, you empower your team to become an active defense mechanism. Every staff member, from interns to executives, has a role in keeping information secure.”

Training as a Strategic Investment

For Kraiger, cybersecurity training is not just a compliance exercise but a strategic business investment. “The cost of a major data breach can cripple an organization financially and reputationally,” he notes. “In contrast, the cost of regular training sessions and awareness programs is modest, and the return on investment is immense.”

Practical training goes beyond one-time presentations or generic online modules. Charles Kraiger advocates for interactive, scenario-based learning that reflects employees' real-world situations. Phishing simulations, password management workshops, and incident response drills all help reinforce best practices.

Building a Culture of Security

Kraiger stresses that awareness is not achieved overnight; it must become part of an organization’s culture. Leaders must set the tone by demonstrating their commitment to security, while managers should reinforce habits that reduce risks. Simple practices like encouraging two-factor authentication, limiting access to sensitive data, and rewarding employees who report suspicious activity create an environment where security is second nature.

“Cybersecurity should be discussed in boardrooms and break rooms,” Kraiger says. “When people

understand that their actions directly impact the organization's safety, they take ownership of their role in protecting it."

Lessons from High-Profile Breaches

Charles Kraiger points to several high-profile breaches where attackers gained entry through phishing campaigns targeting unsuspecting staff. In many cases, attackers didn't need sophisticated hacking tools. They simply tricked someone into handing over credentials. "These incidents remind us that the human element is often the path of least resistance. Attackers exploit trust, distraction, or lack of training. Businesses must address this with proactive education."

The Role of Continuous Education

Cyber threats evolve daily, making one-time training insufficient. Kraiger recommends quarterly refresher courses, monthly security bulletins, and frequent testing to keep knowledge fresh. "Education should be ongoing, just like the threats are ongoing," he explains. "The successful organisations treat cybersecurity as a living, breathing priority."

Preparing for the Future

As artificial intelligence, cloud services, and remote work environments expand, new vulnerabilities will continue to emerge. Charles Kraiger warns that technical defenses will never be enough. "Hackers know that people are the soft targets. Until businesses commit to educating their workforce, they will remain exposed."

His advice to executives is simple: start small, but start now. Implement basic awareness training, evaluate current practices, and build from there. Over time, organisations can create technical and human protection layers that significantly reduce risk.

About Charles Kraiger

Charles Kraiger is a cybersecurity analyst and thought leader with over a decade of experience in cyber threat analysis, risk management, and strategic program development. His career spans senior government roles and advisory work with organizations seeking to strengthen resilience against digital threats. Kraiger combines technical expertise with a passion for leadership and education, helping businesses and institutions navigate the ever-changing cybersecurity landscape.

To learn more visit: https://charles-kraiger.com/

Media Contact

Market News

*********@mail.com

Source : Charles Kraiger

See on IssueWire