Build Organizational Resiliency Through Cyber Training

Michele Vayle | RENOVODATA

ADOBE STOCK/RICHELLE

MORE THAN EVER before, supply chain and logistics organizations are under the constant, unrelenting threat of cyberattacks. Bad actors continue to manufacture highly effective phishing, malware, and ransomware campaigns that target servers, networks – and most importantly – users in the transportation space. The risk associated with third-party logistics companies suffering targeted cyberattacks is magnified, not only by the 24-hour uptime demanded by the industry, but by the exposure that the breadth of essential customers face when 3PL's are infected. Firewalls and anti-malware software exist as investments that can provide some protection, but there is no substitute for training your organization's users so they can recognize and avoid cyberattacks.

Cyberattacks in 2022

- Supply chain was responsible for 62% of System Intrusion incidents in 2022 (Verizon)
- In 2022, 10 million users were impacted by supply chain attacks targeting 1,743 entities. (Helpnet Security)
- Globally, the cost of cybercrime in 2022 was approximately $8.44 trillion. (Statista Cybersecurity Outlook)
- 90% of all enterprise cyber breaches occur because of an unsuspecting employee not being prepared with the basic steps of cybersecurity (ThreatAdvice)
- 71% of cyberattacks in 2022 were initially breached due to "credential compromise", primarily because of simple passwords being used, including accounts used for system administration (Forbes)

Why Invest in Cyber Training

Compared to the risk of having untrained employees expose your organization to the threat of cyberattacks, there is nearly no drawback in an investment in cyber training. Investing in your employees reduces vulnerabilities and drives a culture of ownership and competence. Nearly all employees at each level of a 3PL provider interface with company technology and data in some capacity, and those precious assets are in jeopardy of being compromised without proper education. Leadership must establish a budget for ongoing cyber training initiatives which integrate continuous cybersecurity training for all employees which will drastically improve organizational knowledge on cybersecurity concepts, terminology, and activities associated with implementing best practices. This will help strengthen your overall cyber resilience.

Resiliency Begins with Awareness

Although transportation companies are constantly being targeted by cybercriminals who intend to disrupt and extort business, the average untrained user hardly considers the possibility that they are the prey. It's essential that employees are made aware that they are considered as an important piece of a bad actors puzzle as leadership. Digestible, ongoing user training such as short videos on cybersecurity best practices including: strong passwords, safeguarding work machines and data, critically reviewing emails, and reaching out to IT managers when questions arise have proved effective in reducing the success of coordinated attacks. Don't assume that your employees have knowledge and experience in dealing with cyberattacks, equip them with awareness of their presence, and the tools to combat them. This culture of awareness helps encourage employees to make good choices online.

Education & Evaluation

Workers in transportation are highly committed and attentive to their jobs duties to meet the 24/7 demands of their industry. Considering this, even if an employer offers cybersecurity training and research materials, it's unlikely employees will engage in those resources without incentive. That's why IT leaders must establish an evaluation method to measure engagement and completion of training. It's recommended that management checks in on employee progress to ensure they are engaged and understand the training being presented to them. Industry leaders recommend short quizzes and comprehension checks that map an individual's progress in cyber training, so that management can address any areas in need of improvement.

Simulations

One of the most common and easiest-to-deploy cyberattacks are phishing scams. There was a 61% increase in the rate of phishing attacks in 2022 year over year (CNBC), and they're steadily becoming more sophisticated and difficult to discern from actual business requests. Combatting phishing can be difficult, especially if you are concerned about the base level of knowledge your employees have in recognizing email scams. If your users have completed the aforementioned training and evaluation – it's time to pose a real threat test. Plenty of cybersecurity training organizations have "phishing simulations" that they can deploy to your organization's users to truly test the likelihood of infection due to phishing. The simulations vary from "easily discernable" to more modernly complex. Statistics on how many users interacted with the simulation inappropriately (opened, shared, downloaded) will give IT administrators another measure of user risk in their environment.

GETTY IMAGES/ -WAD-

Resources

Identify training resources, best practices, and frameworks through professional associations, academic institutions, private sector, and government resources including www.CISA.gov. Build a network of trusted relationships with vendor partners like cybersecurity, insurance, and disaster recovery partners to leverage as industry advisors.

Preparation is the Key to Success

Cyberattacks are more complex, relentless, and nefarious than ever before. Quality cloud backups, disaster recovery solutions, security, and planning are important – but they are not a substitute for building a frontline defense by educating and training your employees. It only takes one unequipped employee and a few well-intentioned clicks to allow a bad actor to penetrate your network. Invest in your organizations most important asset – your people – and reduce your risk exposure while increasing your resiliency to cyber threats.