ETHICO

Cybersecurity and Data Confidentiality Training Key to Managing Risks

EDUCATE | MOTIVATE | INFLUENCE

Cybersecurity and data privacy is more important than ever during these uncertain times. Cyber criminals posing as officials from the U.S. Centers for Disease Control and Prevention and the World Health Organization are taking advantage of the COVID-19 emergency. Both agencies posted alerts warning people of phishing emails designed to steal information or trick people into sending money or opening attachments that download malware.

Training employees, including remote workers, on their responsibility to safely access and handle data is important in every industry. Raising awareness of how data and systems can be compromised and how easily and quickly it can happen can be an eye-opener. Organizations that work diligently to protect their systems are only as strong as their weakest link – generally it's their employees.

The cost of cyber crime

With cyber crime hitting $1.5 trillion in revenue in 2018, according to one study, the total cost of cyber crime for each company rose from $11.7 million to $13 million, a 12% increase from 2017 to 2018. The average cost of a single data breach nears $4 million and puts over 25,500 records at risk, according to a 2019 report by Ponemon Institute and IBM Security.

And ransomware attacks — a type of malware that encrypts files and requires the user to make an electronic payment to restore access — are predicted to occur every 11 seconds by 2021, at a cost of $20 billion.

How employees put data at risk

Studies suggest that business owners believe their own employees represent the highest risk of data breaches. In a study done by computer security firm Kaspersky, 52% of respondents said their highest risk is from employees – whether intentional or accidental. The same survey found that, second only to malware, 46% of reported cyber attacks were the result of careless or uninformed staff members.

The BYOD, or bring your own device, trend has made it even more difficult to secure data. With employees accessing company systems from their smartphones, for example, the risk increases. The same Kaspersky study found over

Cybersecurity and Data Confidentiality Training Key to Managing Risks (continued)

one-third of incursions were the result of employees who lost their device; another 48% resulted in careless use of devices. Employees who don't use screen locks to protect their phones, and organizations that don't require additional login security, also put themselves at risk.

Data privacy isn't limited to business information. When employees leave their desks with social media sites logged in and other password-protected sites open, they offer cyber criminals a paved path to their personal data.

Phishing and insider threats

Phishing — tricking someone into revealing information or taking action — is one of the most common attacks using social engineering techniques. Employees who don't scrutinize email addresses of senders and URLs before opening or clicking are most vulnerable.

Insider threats are another source of data incursion. Insider breaches, often from disgruntled employees, are on the rise and accounted for 34% of all breaches in 2018, according to a data breach investigations report by Verizon.

Information security training also raises awareness of the risk that physical papers and files pose, if left unattended, and the importance of keeping contracts, sales records and other confidential and sensitive employee, company and customer information secure.

General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) is a European Union (EU) law that went into effect in 2018. GDPR states that EU citizens have certain rights to their personal data and requires organizations to protect the personal data and privacy of individuals. GDPR applies to organizations, regardless of their geographic location, if they have an EU market, have localized EU web content, and collect personal data from someone in an EU country. With global commerce, everyone who accesses, processes or stores data plays a role in keeping the organization in compliance with GDPR.

Ethico's industry-leading online training courses feature modern, bite-sized episodes presented in a news-style format. Training options include a variety of interactive courses on subjects from Data Privacy, General Data Protection Regulation (GDPR) & Information Security to Code of Conduct, which instruct learners on how to handle difficult, real-world situations and leverage challenge questions to increase learner retention.

ENGAGING & EFFECTIVE FORMAT