Cyber Risks & Liabilities

May/June 2023

4 Reasons Why Cybersecurity Training Fails

Allianz's 2023 risk barometer reported that cyber incidents topped the list of risks facing businesses worldwide in 2023 for the second year in a row, making thorough staff training and a strong cybersecurity culture more important than ever. Indeed, cybercriminals continue to adapt their tactics to exploit victims, and new technologies like ChatGPT could make cyberattacks harder to spot. Therefore, cybersecurity awareness training must include the latest information.

Unfortunately, such training programs aren't always successful, and knowing why can help you avoid similar pitfalls. Consider the following four reasons why cybersecurity training fails:

1. **Training gives limited context**. Many training programs include general cybersecurity guidance rather than industry-specific information. For instance, generic phishing emails (e.g., a fraudulent Netflix account reset email sent to a business address) often form the bulk of training examples, which can disengage employees who don't see the relevance. Instead, include specific training examples, give context to why training sessions are important and explain how teachings fit into broader cybersecurity goals.
2. **Training includes few topics**. Programs often focus too much on phishing. While phishing is a significant threat to businesses and deserves considerable attention, other cyberattack tactics are on the rise. Ensure training incorporates a range of topics, including current trends and regulatory requirements.
3. **Training blames the victim**. Sometimes, training puts the victim at fault for clicking suspicious links or falling for scams. Such notions could make employees less likely to report suspicious behaviour for fear of being criticized. Thus, make sure training supports employees and empowers them to take action.
4. **Training excludes managers**. Training programs may focus on the general workforce and exclude board members or senior leadership. This strategy creates the impression that management is not invested in cybersecurity nor values its importance. Instead, create a culture where cybersecurity is everyone's responsibility.

Contact us today for further cybersecurity guidance.

5 Ways to Reduce Data Exposure

Cybersecurity threats and trends can change year after year as technology advances at alarming speeds. As such, it’s critical to continually reassess your data protection practices. Consider the following five ways to reduce your data exposure:

1. **Install strong antivirus software.** Antivirus software is one of the best ways to protect data. Once installed, keep antivirus programs up to date.

2. **Create strong password policies.** Ongoing password management can help prevent unauthorized attackers from compromising your password-protected information. Require employees to change their passwords regularly and avoid using the same password for multiple accounts.

3. **Use multifactor authentication.** Along with using a complex password, users should be required to confirm their identity with additional information before access to corporate networks is granted.

4. **Patch systems regularly.** Update operating systems, software and firmware frequently to prevent cybercriminals from exploiting software vulnerabilities.

5. **Back up data.** Secure business-critical data by keeping backup files in case the system is compromised.

Understand the Risks of Third-party Service Providers

As business processes expand in complexity, organizations turn to third parties to help provide critical services and remain competitive. Furthermore, during tough economic times, organizations may consider outsourcing labour-intensive work in order to save money.

However, the use of third-party services comes with significant cybersecurity risks. Specifically, cybercriminals could breach a supplier’s network perimeter and attack your organization through lateral movement. Indirect cyberattacks of this nature have risen over the past few years from 44% to 61%, according to a Global Cybersecurity Outlook 2022 report. Consider the following risks of using third-party service providers:

- **Reputational damages**—Should one of your suppliers experience a cyber breach, your reputation could be on the line. Specifically, your organization could come under scrutiny due to the mere association with the affected company. Consequently, concerned customers may leave for other providers and financial losses and other issues could stem from your damaged reputation.
- **Compliance concerns**—Managing your supply chain risk is vital to adhere to all relevant data protection regulations. For instance, a third-party customer relationship management provider that retains your customers’ contact details may fall under the scope of your own Personal Information Protection and Electronic Documents Act (PIPEDA) compliance. As such, you could suffer financial penalties for failing to comply with appropriate regulations if a supplier experiences a cybersecurity breach.
- **Operational issues**—If a software vendor experiences a cyberattack, your services could be left offline for significant periods. Extensive downtime may result in productivity losses and a damaged reputation.

To avoid these and other risks, it’s essential to vet all third-party suppliers before granting them access to your IT systems. It’s worth noting that while vendors may have adequate safety protocols at first, they may not always retain them. Therefore, it’s important to rigorously monitor a third-party supplier’s performance and security measures for the duration of your dealings with them. Additionally, only work with vendors who have responsible security safeguards, business continuity plans and disaster recovery strategies.

For further risk management strategies and guidance, contact us today.