Allianz’s 2023 risk barometer reported that cyber-incidents topped the list of risks facing businesses around the world in 2023 for the second year in a row, making thorough staff training and a strong cyber-security culture more important than ever. Indeed, cyber-criminals continue to adapt their tactics to exploit victims, and new technologies like ChatGPT could make cyber-attacks harder to spot. Therefore, cyber-security awareness training must include the latest tips and trends.

4 Reasons Why Cyber-security Training Fails

**Best Practices to Keep Routers Secure**

Most homes and offices have a router that provides internet access to multiple devices within the same space. Unfortunately, cyber-criminals may target routers because they can steal data or alter a router’s ability to recognise illegitimate websites, putting users and their organisations at risk. Employees working from home may be particularly vulnerable to cyber-attacks via routers. As such, it’s important for organisations to share the following best practices with staff:

**Best Practices to Keep Routers Secure**

Most homes and offices have a router that provides internet access to multiple devices within the same space. Unfortunately, cyber-criminals may target routers because they can steal data or alter a router’s ability to recognise illegitimate websites, putting users and their organisations at risk. Employees working from home may be particularly vulnerable to cyber-attacks via routers. As such, it’s important for organisations to share the following best practices with

**5 Ways to Reduce Your Data Exposure**

Cyber-security threats and trends can change year over year as technology continues to advance at alarming speeds. As such, it’s critical that you continually reassess your data protection practices. Consider the following five ways to reduce your data exposures:

1. **Install strong antivirus software.** Antivirus software is one of the best ways to protect your data. Once installed, keep antivirus programs up to date.
2. **Create strong password policies.** Ongoing password management can help prevent unauthorised attackers from compromising your password-protected information. Require employees to change their password on a regular basis and avoid using the same password for multiple accounts.
3. **Use multi-factor authentication.** Alongside a complex password, require users to confirm their identity with additional information before allowing access to corporate networks.
4. **Patch systems regularly.** Update operating systems, software and firmware frequently to prevent cyber-criminals from exploiting software vulnerabilities.
5. **Backup data.** Secure business critical data by keeping backup files in case your system is ever compromised.

Unfortunately, such training programmes aren’t always successful, and knowing why can help you avoid similar pitfalls. Consider the following four reasons why cyber-security training fails:

1. **Training gives limited context**. Many training programmes include general cyber-security guidance rather than industry-specific information. For instance, generic phishing emails (eg 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 cyber-security goals.
2. **Training includes few topics**. Programmes often focus too much on phishing. While phishing is a significant threat to businesses and deserves considerable attention, other cyber-attack 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 criticised. Thus, make sure training supports employees and empowers them to take action.
4. **Training excludes managers**. Training programmes may focus on the general workforce and exclude board members or senior leadership. This strategy creates the impression that management is not invested in cyber-security nor values its importance. Therefore, it’s essential to create a culture where cyber-security is everyone’s responsibility.

Even if your training programme is strong, it may not be effective if employees who breach your company’s IT policy don’t face consequences. Make clear to staff the repercussions of lax security.

Contact us today for further cyber-security guidance.

**5 Ways to Reduce Your Data Exposure**

Cyber-security 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 programmes up to date.
2. **Create strong password policies.** Ongoing password management can help prevent unauthorised attackers from compromising your password-protected information. Require employees to change their password on a regular basis 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 cyber-criminals 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, organisations turn to third parties to help provide critical services and remain competitive. In fact, 7 in 10 British businesses outsource to third parties, according to a YouGov survey. This statistic could increase during tough economic times as organisations consider outsourcing labour-intensive work in order to save money.

However, the use of third-party services comes with significant cyber-security risks. Specifically, cyber-criminals could breach a supplier’s network perimeter and attack your organisation through lateral movement. Indirect cyber-attacks of this nature have risen over the past few years from 44% to 61%, according to a Global Cyber Security 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 organisation 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**—Regulators are increasing the pressure on organisations to better manage their supply chain risk. For instance, a third-party customer relationship management provider that retains your customers’ contact details may fall under the scope of your own General Data Protection Regulation compliance. As such, you could suffer financial penalties for failing to comply with appropriate regulations if a supplier experiences a cyber-security breach.
* **Operational issues**—If a software vendor experiences a cyber-attack, 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 nothing 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.