MACKAY
Corporate Insurance Brokers

CYBER-RISKS & LIABILITIES

Q2 2026

Improving the Effectiveness of Cyber-security Training

People remain the most common point of entry for cyber-incidents, regardless of how strong an organisation's technical controls may be. In fact, according to a report by Verizon, more than two-thirds of data breaches involve human error. Despite this, many cyber-security training programmes fall short. Too often, they function as a "tick box" exercise—delivering information without driving meaningful behavioural change. While employees may learn about common threats, they are not always equipped to apply that knowledge in real-world situations.

To make training more effective, organisations should consider the following strategies:

- **Leverage storytelling**. Using real-world incidents can make training more relatable and memorable. Stories that illustrate how small mistakes led to significant consequences can help employees better understand the real-world impact of their decisions. Training scenarios should be adapted to the specific responsibilities, risks and experience levels of different employee groups; for instance, finance teams may benefit from stories involving invoice-related phishing scams, while IT teams could explore scenarios that highlight insider-threat indicators or unusual system activity.
- **Provide hands-on learning**. Interactive approaches, such as simulated phishing attacks, workshops, or role-play scenarios, allow employees to practise identifying and responding to threats in real time. Hands-on learning allows employees to apply what they have learnt from static training materials and reinforce key behaviours through practical experience. These exercises also generate valuable data, such as how many employees engaged with a phishing attempt, which organisations can use to refine future training.
- **Consider gamification**. Incorporating elements like rewards, friendly competition and progress tracking can make training feel more engaging and less like a compliance requirement. Gamified training encourages repeated interaction and helps reinforce learning over time. For example, short phishing-spotting challenges or team-based activities can reinforce specific behaviours, such as identifying suspicious links or verifying unusual requests.

For training to be fully effective, organisations should reinforce it with a culture of accountability and robust leadership support.

Steps to Take When Responding to a Data Breach

No organisation is immune to cyber-threats, and data breaches can affect businesses of any size or sector. A data breach involves the unauthorised access, loss or disclosure of sensitive information—whether through malicious activity, such as ransomware, or human error, like sending data to the wrong recipient.

When a breach occurs, a prompt and structured response is essential to minimise damage and meet regulatory obligations. Organisations should act quickly to contain the incident and begin an internal investigation. This includes alerting IT or cyber-security teams, preserving evidence and documenting key details, such as when the breach occurred, which systems were affected and what data may have been compromised. Organisations must also assess the potential risk to individuals. If the breach poses a high risk to people's rights and freedoms, it should be reported to the Information Commissioner's Office within 72 hours, and affected individuals must be informed without undue delay. Even where reporting is not required, all breaches should be recorded internally. A clear, consistent response process helps support compliance and reduce future risks.

Contact us today for additional cyber-security guidance.

Understanding SEO Poisoning Attacks

Search engines are a trusted tool for finding information quickly. However, that trust is increasingly being exploited through a growing cyber-threat known as search engine optimisation (SEO) poisoning. In these attacks, cyber-criminals manipulate search rankings to push malicious or compromised websites to the top of results, where users are more likely to click.

For organisations, the risk is significant. Employees who unknowingly interact with malicious search results may download malware, disclose credentials or grant unauthorised access to systems—potentially leading to financial losses, data breaches and reputational damage.

SEO poisoning turns trusted search results into hidden threats. By manipulating rankings, cyber-criminals lure users to malicious sites—making awareness, verification habits and strong technical controls essential for protecting organisational data and systems.

SEO poisoning works by exploiting legitimate optimisation techniques. While SEO is typically used to improve visibility, attackers abuse it to promote harmful content. Common tactics include keyword stuffing, where malicious pages are overloaded with popular search terms; compromising legitimate websites to insert malicious links; and creating networks of low-quality sites (link farms) to artificially boost rankings.

Other methods include cloaking—showing safe content to search engines while delivering malicious content to users—and typosquatting, where attackers create look-alike domains to trick users into visiting fraudulent sites

Unlike traditional “push” attacks, such as phishing emails, SEO poisoning is a “pull” attack. Users actively seek information and are drawn in by seemingly legitimate results, making these threats harder to detect and avoid.

Once users click a poisoned result, they may be redirected to phishing pages, prompted to download malicious software or asked to enter sensitive information into fake portals. In some cases, attackers can gain a foothold within a system, enabling further activity such as ransomware deployment or data exfiltration.

To reduce exposure to SEO poisoning, organisations should take a proactive approach by implementing the following:

- **Strengthen website security** by using HTTPS, enforcing strong passwords and multifactor authentication, and regularly updating systems and plugins.
- **Monitor for suspicious changes**, including unexpected content, unusual links or unexplained shifts in search rankings.
- **Watch for brand impersonation** by tracking look-alike domains and encouraging employees to use trusted bookmarks or official portals.
- **Implement technical controls**, such as web filtering, endpoint protection and network monitoring to detect unusual activity.
- **Train employees on safe searching**, including verifying URLs and avoiding reliance on search results for sensitive actions like downloading software.

SEO poisoning highlights how cyber-risks continue to evolve. By combining technical safeguards with employee awareness, organisations can better defend against this increasingly sophisticated threat.

Contact us today for further guidance on cyber-risk management.

Contains public sector information published by the ICO and NCSC and licensed under the Open Government Licence v3.0.
The content of this publication is of general interest and is not intended to apply to specific circumstances or jurisdiction. It does not purport to be a comprehensive analysis of all matters relevant to its subject matter. The content should not, therefore, be regarded as constituting legal advice and not be relied upon as such. In relation to any particular problem which they may have, readers are advised to seek specific advice from their own legal counsel. Further, the law may have changed since first publication and the reader is cautioned accordingly.
© 2025 Zywave, Inc. All rights reserved.