MACKAY
Corporate Insurance Brokers

CYBER-RISKS & LIABILITIES

Q3 2026

Fostering a Cyber-security Culture

Employees remain one of the most common targets of cyber-attacks, making them an organisation's first line of defence. Yet many incidents still result from human error, whether through phishing scams, weak passwords or mishandling sensitive information. As such, cyber-security should be more than a technical concern—it should be embedded within workplace culture.

Creating a strong cyber-security culture is not a one-time initiative. It requires ongoing communication, regular training and consistent reinforcement across all levels of the organisation. When employees understand that cyber-security is part of their everyday responsibilities, they are more likely to recognise potential threats and make informed decisions that help protect business systems and data.

To foster a strong cyber-security culture, consider the following practices:

- **Lead from the top.** Senior leaders should demonstrate a visible commitment to cyber-security and reinforce its importance through their actions.
- **Encourage accountability.** Employees should understand how their decisions can affect organisational security and what steps they can take to reduce risk.
- **Promote good cyber-hygiene.** Organisations should regularly reinforce fundamental practices such as strong passwords, multifactor authentication and safe internet use.
- **Support secure communication.** Organisations should ensure employees know how to report suspicious messages and verify the legitimacy of work-related communications.
- **Recognise positive behaviour.** Organisations should reward good cyber-security practices to encourage long-term engagement.

By making cyber-security a shared responsibility, organisations can strengthen their resilience against evolving threats and reduce the likelihood of costly cyber-incidents.

Understanding Zero Trust Architecture

The rise of hybrid working has transformed how employees access business systems and data. Traditional security models often assume that users and devices inside an organisation's network can be trusted. However, this approach is becoming less effective as organisations rely on cloud services, remote access and mobile devices.

Zero trust architecture (ZTA) takes a different approach. Rather than automatically trusting users or devices based on their location, ZTA assumes that no one should be trusted by default. Every access request must be verified using factors such as identity, device health and user permissions before access is granted.

Zero trust does not mean eliminating trust altogether. Rather, it means continuously verifying trust. Access decisions are based on current information, helping organisations ensure that users receive only the permissions they need and that access can be adjusted quickly if risks or circumstances change.

This approach can help organisations reduce the risk of unauthorised access, limit the impact of compromised accounts and improve overall cyber-resilience. The UK's National Cyber Security Centre recently published new guidance on designing secure access using zero trust network access, helping organisations adopt these principles in modern working environments.

Contact us today for additional cyber-security guidance.

LLMjacking Cyber-attacks Explained

As artificial intelligence (AI) tools become increasingly common in business operations, cyber-criminals are finding new ways to exploit them. One emerging threat is LLMjacking, a cyber-attack in which criminals steal credentials used to access large language model (LLM) platforms and then use those accounts for their own purposes.

LLMjacking typically begins when attackers obtain AI platform credentials through phishing campaigns, exposed code repositories, software vulnerabilities or stolen credentials purchased online. Once they gain access, they can use the victim's account to generate spam, create malicious code, support social engineering attacks or resell access to other criminals. Because this activity often resembles legitimate usage, organisations may not discover the attack until they receive unusually high usage charges or warnings from their AI provider.

Many AI providers offer spending alerts, usage monitoring tools and configurable usage caps, making proactive account monitoring an important defence against unexpected costs and unauthorised activity.

The growing popularity of AI tools has made LLMjacking particularly attractive to cyber-criminals. Unlike many traditional cyber-attacks, LLMjacking does not require attackers to infiltrate an organisation's internal network. Instead, they can exploit legitimate credentials to access valuable AI resources directly. As businesses increasingly integrate AI into customer service, software development, data analysis and other core functions, compromised AI accounts can provide attackers with both financial opportunities and access to sensitive information.

Business Impacts of LLMJacking

The consequences of LLMjacking can be significant. Businesses may face substantial financial losses from unauthorised AI usage, operational disruptions if account limits are exhausted, and potential exposure of sensitive business information. In some situations, organisations may also encounter regulatory scrutiny, legal liability and reputational damage if compromised accounts are linked to harmful or unlawful activity.

The risk is expected to grow as AI adoption accelerates across industries. Many organisations have implemented AI tools more quickly than they have established governance and security controls around them. As a result, AI credentials may not receive the same level of protection as other critical business systems, creating opportunities for cyber-criminals to exploit overlooked vulnerabilities.

Reducing the Risk

To reduce the risk of LLMjacking, organisations should protect AI credentials using secure credential management tools, enforce least-privilege access controls, and regularly rotate login credentials and access keys. It is also important to monitor AI platform activity for unusual usage patterns, unexpected access locations or sudden spikes in costs. Employee training should address AI-specific risks and emphasise the importance of safeguarding platform credentials. Additionally, incident response plans should include procedures for responding to compromised AI accounts.

Insurance can also play a role in managing LLMjacking exposures. Depending on policy terms, cyber-insurance may help cover costs associated with unauthorised usage, business interruption, data compromise and incident response activities. However, cover varies between insurers, making it important to review policies carefully and address any gaps.

As AI tools become more deeply integrated into business operations, the credentials that power them are becoming increasingly valuable targets. By understanding LLMjacking and implementing appropriate safeguards, organisations can better protect their AI investments and reduce the likelihood of costly cyber-incidents.

Contact us today for more risk management guidance and insurance solutions.