MACKAY
Corporate Insurance Brokers

CYBER-RISKS & LIABILITIES

November/December 2025

Managing Zero-click Attacks

While most cyber-attacks involve users being manipulated into taking specific actions—whether it's sharing login credentials, downloading dangerous attachments or clicking on harmful links—some incidents can be launched without these exchanges. In particular, zero-click attacks involve hackers exploiting software flaws in devices and applications to deploy malicious code, all without requiring any user interaction. As cyber-threats grow increasingly sophisticated, these silent intrusions are becoming more prevalent, marking a new frontier in security risks for organisations across sectors.

Zero-click attacks can affect organisations in many ways, leading to stolen assets, damaged systems and regulatory penalties. As such, companies should consider the following risk mitigation measures:

- **Maintain updated software**. Employers should make it a priority to regularly update all workplace devices, operating systems, applications and firmware. Timely updates help patch known vulnerabilities and reduce the risk of cyber-criminals exploiting outdated technology.
- **Utilise multi-layered security solutions**. All company devices should be equipped with advanced threat identification systems, antivirus programs, firewalls and intrusion detection tools to improve visibility across IT infrastructure and detect abnormal activity.
- **Establish segmented networks**. Organisations' networks should be segmented to prevent cyber-criminals from travelling laterally through their systems. This way, hackers will only be able to compromise a small portion of corporate resources at a time, minimising the risk of large-scale damage.
- **Vet all vendors and applications**. Employers should thoroughly assess all third-party software vendors and the applications they provide, especially niche or lesser-known ones, for potential security vulnerabilities before entering into any agreements.

Securing Mobile Devices in the Workplace

Mobile devices, including smartphones and tablets, play a critical role in enabling productivity and facilitating communication. However, when used to access or store sensitive corporate information (eg emails and proprietary data), these devices can expose organisations to significant risk. Specifically, mobile devices can be misplaced or stolen, and cyber-criminals may gain unauthorised access to sensitive data, especially if password protocols are weak or biometric protections are improperly configured. Threats can also arise if employees connect devices to unsecured wi-fi networks, which can expose data to interception, malware injection or man-in-the-middle attacks.

Organisations can reduce security risks by enforcing clear mobile device usage policies and providing employees with targeted training on how to protect sensitive data. Companies should also ensure regular data backups, enforce strong password practices, and install tools that allow remote locking or wiping of compromised devices. Keeping software and antivirus programs up to date can further strengthen an organisation's defences against evolving threats.

In today's increasingly device-driven work environments, prioritising mobile security is essential. Whether employees use company-issued or personal devices, organisations must set robust security standards to protect sensitive data, maintain trust and reduce the risk of costly breaches.

Contact us today for additional cyber-security guidance.

Understanding Shadow IT: Benefits, Risks and Management

As digital transformation accelerates, employees are increasingly adopting tools and technologies outside the purview of their organisation's IT department. Whether it's using personal devices to access corporate systems, personal cloud storage to share files or unapproved software to streamline tasks, this unsanctioned use of technology—known as shadow IT—has become widespread. The rise of remote and hybrid working models has intensified this trend, as unsupervised environments make it easier for staff to bypass established security protocols.

Despite the risks, shadow IT can offer benefits. It enables teams to adopt innovative solutions quickly, bypassing lengthy IT approval processes and boosting productivity. It can also improve employee satisfaction by giving individuals greater control over their digital tools. In some cases, it may even reduce costs by leveraging free or low-cost software and enabling bring-your-own-device practices.

While often driven by a desire for efficiency and flexibility, shadow IT can create significant blind spots in an organisation's security posture, potentially exposing it to data security and regulatory compliance risks.

However, the downsides are significant. Shadow IT can lead to:

- **Security gaps**—Shadow IT undermines an organisation's control over its digital environment. Unvetted tools fall outside standard cyber-hygiene measures (eg antivirus protection and threat monitoring), raising the risk of data breaches.
- **Data loss and leakage—**Shadow IT threatens data integrity and access. Sensitive information shared via unsecured channels could be exposed, and data held in personal accounts may be lost if an employee departs, disrupting operations.
- **Loss of visibility and control—**Shadow IT limits IT teams' ability to enforce policies, manage access and apply updates, leaving systems exposed to cyber-threats and organisations at risk of regulatory breaches. Unmanaged tools can also malfunction, causing disruptions to operations.
- **Increased costs and redundancy—**Duplicate or overlapping services drain resources and complicate support. Untracked tools may lead to unnecessary spending and inconsistent software use, decreasing collaboration and productivity.
- **Reputational damage**—Breaches, performance issues and compliance failures linked to shadow IT can harm brand credibility, trigger customer complaints and erode stakeholder trust.

To manage these risks, employers should establish clear, company-wide usage and procurement policies to curb shadow IT. Policies should define acceptable use of third-party applications and devices, set restrictions on unsanctioned software and create transparent approval mechanisms.

Moreover, organisations should regularly audit network and cloud activity to uncover unauthorised tools and hidden assets. These audits should be supported by broader IT assessments that incorporate staff feedback, help desk logs and expense reports. Additionally, implementing strong access controls—such as multi-factor authentication and network segmentation—can help reduce exposure to threats. Staff training is also essential to educate employees about the risks of using unapproved applications, devices and software.

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