MACKAY
Corporate Insurance Brokers

CYBER-RISKS & LIABILITIES

May/June 2025

Understanding SIM-swapping Attacks

In recent years, a growing number of organisations have implemented stronger cyber-security measures, including multifactor authentication (MFA). This method requires users to present two or more unique credentials, such as a password and an additional security code, to verify their identity and log into their company account.

However, some cyber-criminals have figured out a way to exploit MFA through users' subscriber identity module (SIM) cards. Specifically, threat actors have begun tricking mobile carriers into transferring users' profiles to SIM cards on their own devices—known as SIM-swapping attacks—thus giving them unauthorised access to users' mobile phone activities. Because the additional security codes required for MFA are often sent via text, cyber-criminals with fraudulent SIM cards can complete users' extra account verification steps with ease and infiltrate company networks, data and funds. To help prevent this type of attack in their organisations, employers should consider the following strategies:

- **Ensure sufficient account security measures.** Cyber-criminals need users' passwords before they can deploy SIM-swapping attacks and exploit MFA. Therefore, organisations must ensure employees create complex and unique passwords.
- **Leverage alternative MFA options.** Because SIM-swapping attacks often rely on MFA-related requests being sent via text, organisations should explore other account verification options that cyber-criminals can't access through a stolen mobile profile (eg face or fingerprint scanning).
- **Protect personal details.** Employers should encourage employees to protect their personal details by keeping their social media accounts private and refraining from sharing this information over text or email, especially with unknown or suspicious recipients. This can make it harder for cyber-criminals to obtain the information needed to trick mobile carriers into conducting a SIM swap.
- **Educate employees.** Employers should train their employees on SIM-swapping attacks, detection and related incident reporting protocols.

Finally, employers should purchase adequate insurance to maintain much-needed financial protection against losses that may arise from SIM-swapping incidents and other cyber-threats. Contact us today to find out more.

Reducing the Risk of Unauthorised Social Media Content

A company's reputation can take years to build but can be damaged quickly. Just one harmful social media post can erode consumer trust and even lead to boycotted products or services. Whether employees draft inaccurate social media messages in error or intentionally attempt to spread misinformation, employers must take steps to reduce the likelihood of damaging social media content getting posted online. Consider these tips:

- **Organisations should implement a content workflow** to manage content creation, approval and publication and ensure that a senior staff member reviews social media posts before they are posted.
- **Organisations should implement a sound password policy and two-step verification** to ensure that only employees authorised to publish social media content gain access to accounts.
- **Social media staff must only use work devices when creating and publishing content**, as they may inadvertently publish content intended for their personal channels when using their own devices.

Additionally, organisations should evaluate any associated cyber-security risks when choosing social media platforms.

Mitigating the Risk of Formjacking

As businesses increasingly rely on online transactions, cyber-criminals have developed a scheme to exploit this process and steal sensitive information. This growing cyber-threat, known as formjacking, poses significant risks to businesses; it is difficult to prevent and can lead to major financial losses and reputational damage.

Formjacking is a cyber-attack method in which a threat actor injects malicious JavaScript into a website, often one that contains an online payment form. Once the targeted page has been compromised, the added code allows the hacker to collect sensitive data, such as credit card numbers, addresses and phone numbers. This data is sent to the cyber-attacker's domain after unsuspecting users enter their information and click "submit" to complete a transaction. Malicious actors can then use the stolen data in identity theft schemes, payment card fraud scams and account takeover attacks, or they can sell it to other criminals. Stolen information can also be used to create fraudulent accounts and distribute malware. The hacker's code may be loaded through various methods, such as by exploiting a vulnerability in a business's website, employing a phishing scam in which the cyber-intruder gains access to a company's checkout page, or compromising a third party's app or JavaScript used by a business.

Approximately 5,000 websites are compromised with malicious formjacking code each month, according to software company Symantec. Formjacking attacks can damage an organisation's reputation and result in regulatory penalties.

Although detecting malicious formjacking code and preventing attacks can be difficult, there are several measures businesses can take to identify potential issues and reduce the risk of this cyber-threat. Organisations can consider these four strategies:

1. **Practise cyber-hygiene.** Organisations should keep software, patches and extensions up to date. Establishing a content security policy and using firewalls and subresource integrity tags can also help prevent the injection of malicious data onto business websites.
2. **Scan and audit website code regularly.** Organisations should frequently scan and audit website code to check its integrity. Furthermore, monitoring and analysing web logs and JavaScript behaviour can help organisations detect malicious activity, and checking where a browser is sending data is also key in stopping formjacking attacks.
3. **Utilise cyber-defence techniques.** Organisations should leverage cyber-defence measures such as obfuscating JavaScript to make code more difficult for cyber-attackers to understand. Implementing network segmentation can also limit network exposures and malicious actors' lateral movement capabilities.
4. **Implement ongoing cyber-security measures.** Organisations can limit exposures by thoroughly testing websites before they are publicly launched, executing penetration testing to discover vulnerabilities, and monitoring the supply chain to ensure vendors whose code is being used follow cyber-security best practices.

Layering defences can also reduce an organisation's vulnerability, and companies should consider leveraging artificial intelligence to help detect suspicious behaviour.

Contact us today for additional cyber-risk management information and robust insurance solutions.