Cyber-risks and Liabilities

September/October 2023

Deepfakes Explained

Deepfakes refer to sophisticated forgeries of an image, video or audio recording using artificial intelligence (AI). As technology has evolved, deepfakes are now able to alter media so well that it's often difficult to detect that any manipulation has occurred. In fact, 95% of people were unable to tell a fake AI-generated voice from a real one in recent research by software company McAfee. There are several types of deepfake attacks organisations should be aware of, including:

- **Scams and hoaxes**—Cyber-criminals may leverage deepfake technology to create scams or hoaxes to undermine organisations. For instance, a criminal could create a false video of a CEO admitting to criminal activity, destabilising the organisation's reputation in the process.
- **Identity theft**—Deepfake technology can be used to give credibility to synthetic identities or clone existing ones. Criminals can then use these identities for nefarious purposes.
- **Social engineering**—Social engineering consists of cyber-criminals convincing victims to make a mistake or compromise sensitive data. When coupled with deepfake technology, fraudsters can easily fool victims into believing that trusted individuals have asked them to do something. For instance, the CEO of a UK-based energy firm thought they were speaking to the chief executive of a partner company, who asked them to send funds to a supplier over the phone. The deepfake was so convincing that the CEO transferred approximately £200,000 to criminals, according to the organisation's insurance firm, Euler Hermes Group SA.

To protect organisations from deepfake schemes, employers can consider the following strategies:

- **Train employees**. Educate employees on deepfakes, including what they are and how they might be used against the business.
- **Utilise detection software.** The earlier deepfakes are detected, the quicker action can be taken to reduce harm. Leverage technology solutions to detect potential deepfake attacks.
- **Establish a response strategy**. Develop a response strategy that details escalation practices and individual responsibilities should a deepfake attack occur.

For further cyber-security and risk mitigation strategies, contact us today.

The Key Benefits of Cyber-insurance

Cyber-security risks continue to evolve each year alongside technological advancements. The development of AI and the rapid growth of Internet of Things devices have increased the ways that cyber-criminals can attack. In fact, 32% of businesses and 24% of charities experienced a cyber-attack in the past 12 months, according to government data. As such, the value of a robust cyber-insurance policy continues to grow. Consider the following benefits of cyber-insurance:

Business interruption loss cover—If an organisation experiences an IT failure or cyber-attack that disrupts operations, its insurer may cover lost income during the interruption.

Cyber-extortion protection—A policy may provide cover in the event that an organisation is infected by ransomware or another malicious software and a fee is demanded from criminals to restore operations.

Digital asset replacement expenses—If an organisation's digital assets are lost or corrupted, its policy may cover the associated costs.

Forensic support—Immediate 24/7 support from cyber-specialists following a hack or data breach may be included in a policy.

Prevention of reputational damage—A policy may help an organisation recoup lost profits directly attributable to cyber-attacks.

Contact us today to discuss robust cyber-insurance solutions.

The Risk of Shadow IT

Shadow IT is the unauthorised use of IT-related devices, software or services without prior agreement from the IT department. For instance, employees might use personal laptops to access work applications, download software to complete work duties, or store work data on personal cloud accounts without asking the IT department first. Although a small amount of shadow IT is expected, larger amounts make it difficult for organisations to understand their risk landscape and protect themselves from cyber-threats. Specifically, shadow IT "unknown assets" are not accounted for by asset management nor aligned with IT security policies and processes. Consequently, organisations could be left vulnerable to data breaches, non-compliance concerns and other cyber-threats.

Typically, shadow IT isn't the result of intentional rule-breaking by staff. Instead, employees seek means to get their jobs done more efficiently without realising the methods used (eg downloading a specific software they use successfully at home) could put their organisations at risk. To mitigate this risk, organisations should consider the following strategies:

- **Avoid unnecessary lockdowns of enterprise IT**. Ensuring employees have the tools they need to do their jobs is important. For instance, if staff don't have an instant messaging platform, they may download software to help them collaborate with colleagues. To prevent this, proactively anticipate users' needs and ensure they have sufficient devices, software and tools to complete work duties.
- **Implement a simple users' request system**. Make it easy for employees to request technology solutions for work demands. This way, they won't feel the need to try and fix problems themselves.
- **Develop a cyber-security culture**. Reinforce the importance of open communication regarding IT and security issues. Make it apparent that employees won't be reprimanded should they raise security concerns, including shadow IT instances.
- **Implement technical controls**. Consider technical mitigations such as strong network access controls to prevent employees from connecting unsanctioned devices and network scanners to identify devices and make comparisons to known assets.

When organisations' IT departments don't know what services and applications are in use, serious security gaps could result. As such, the risk of shadow IT must be considered by all organisations, and appropriate risk mitigation strategies should be implemented to bolster security efforts.

For additional cyber-security resources, contact us today.