sioma

Cyber Insurance – Example of Claims

Ransomware Attacks

Ransomware is the most common cyber insurance claim. Ransomware is a type of malware that a threat actor uses to encrypts your files, so you are unable to access your device, and the data stored on it. Once they have access to your system, they (threat actors) can sit dormant for months before they decide to encrypt your files. During this time, they are watching what you're doing on your device and collecting data, waiting for the right time to strike before demanding a ransom in exchange for decryption or threaten to leak the stolen data.

Ransomware can gain access to your business in several ways, including:

- Phishing – If an employee clicks on a malicious link within a seemingly genuine email, allowing ransomware to infiltrate.
- Remote Desktop Protocol (RDP)
- No VPN or MFA used - Threat actors gain access to the network using a brute force attack as only a simple password was preventing access, and no VPN used to 'hide' the client's network.
- Unpatched VPN/RDP/software – When software is not regularly updated with the latest security patches and leaves a vulnerability in the network. Threat actors take advantage of this and gain access, installing ransomware and/or stealing data.

Funds Transfer Fraud

CEO fraud (or Friday fraud) is a type of attack in which a cybercriminal impersonates an employee with the power to ask employees to make payments. This could be a CEO, CFO, Head of HR, etc. The email will usually contain an invoice from a supplier which contains new account details. An employee in accounts receives a seemingly genuine email from the boss or a known customer at the last-minute requesting urgent payment of an invoice.

Vishing

Vishing scams are when scammers will impersonate a legitimate source in an attempt to extort money. An example of a vishing scam is a call from the "bank" stating that your account has been compromised and that immediate action is required. Usually, this action includes transferring bank details and security information to the threat actor.

Dependent Business Interruption Loss

A third-party service provider goes down unexpectedly as a result of a 'cyber event', meaning that the insured is unable to work as they lose access to their computer networks.

Denial of Service Attack

A denial-of-service attack is when a threat actor attempts to disrupt a computer or other device's normal functioning and make the device inaccessible to users.

During this malicious attack, the threat actor overwhelms a website with traffic, resulting in the website, and/or sales, going down. They typically do this during a busy sales period, preventing the insured from being able to trade. Sometimes a ransom is attached to cease action.

Rogue Employee

A rogue employee is a member of staff who harms their company by engaging in illicit activity, e.g., a worker collects sensitive and confidential data over time with a view to selling. As part of General Data Protection Regulation (GDPR), all organisations must report data breaches to the Information Commissioner's Office (ICO) and individuals impacted by the data breach. This opens a door for individuals to seek financial compensation as a result.

Rogue employees tend to fall into one of three categories:

- Ambitious – Cuts corners regarding cyber security best practices to get things done as quickly as possible.
- Disgruntled – Intends to subvert cyber security practices as a form of backlash against their employers.
- Negligent – Breaks cyber security best practices because they simply do not care about the consequences.

*This content was sourced and adapted from Towergate. Thank you to our insurance partners at Towergate for providing these helpful examples and insights, which we've tailored for our website.

sioma

0204 586 1202

Floor 3

38 South Molton Street

London

W1K 5RL

www.sioma.co.uk

Boutique Insurance Advisory

British Insurance Brokers' Association

FCA FINANCIAL CONDUCT AUTHORITY

Chartered Insurance Institute