Claims Examples

EMERGENCE

Cyber Insurance helps the insureds business recover after a cyberattack or a data breach. Organisations are increasingly reliant on technology. With ever more digital products and services, businesses are ever more in need of cyber protection.

Our Cyber Event Protection Insurance provides comprehensive cover:

- Protection against a drop in Revenue
- Response Costs and support to get the insureds business back in business
- Protection against 3rd Party Liability
- Cyber Theft and Telephone Phreaking Protection
- Protection against Tangible Property Damage

Example	Claim Scenario	Cyber Event Protection Solution
Extortion Attempt	A malicious person pretending to be tech support gained access to the insured's computer systems. This enabled them to pose as an insider, eventually gaining access to highly restricted information including customer trade secrets, bank details and other sensitive personal information. The hacker threatened to sell trade secrets to competitors and banking details on the black market, and make sensitive personal information public - unless the insured paid.	Cyber Event Protection provides coverage for key areas of loss including: forensics, crisis management and public relations, notification costs, and credit and identity monitoring. The policy covers costs as a consequence of a mandatory notice from a regulatory authority because of the insured's failure to secure information held. Defence and settlement costs for 3rd party claims made against the insured are also covered, as well as impact on business costs, based on revenue shortfall during the indemnity period, if any.
CryptoLocker Attack	An employee clicks on a plausible email attachment which unleashes a CryptoLocker virus. This prevents the insured operating their systems.	Cyber Event Protections provides coverage for IT Forensic technicians to remove the virus and mitigate further threats to the insureds systems. Business interruption and extra operating expense as a result of the breach are also covered.
Hacking	The insured operates an e-commerce website which becomes infected with malicious code. Customers and staff are unable to access orders in the system as the website shows a black screen.	The policy will provide coverage for revenue impacts on the insureds business as a result of the Cyber Event. Defence costs, awards, fines or penalties to customers affected are covered, as well as costs to restore the website. Business interruption and extra operating expense as a result of the breach are also covered.
Phone Phreaking	The insured suffered a breach resulting in unauthorised international calls being made through their phone system. The unknown person created a mailbox to route calls overseas.	This coverage pays for the appointment of forensics investigators who will investigate and remove the threat to the insureds business. Our Cyber Theft optional coverage pays the direct financial loss to the insured.
Social Engineering Fraud Business e-mail Compromise 1st part loss	The CFO receives a fraudulent email from the CEO, whose e-mail account has been compromised, requesting the transfer of a large sum of money. The email convinced the CFO to transfer the money to a third party bank account. Later it's determined the email was not authored by the CEO, but it's too late for the bank to stop the transfer.	Cyber Event Protection will cover for the insureds Cyber Event response costs to remove the threat and secure the e-mail system. If Cyber Theft coverage is applicable, the direct financial loss the insured suffered will be covered as well.
Social Engineering Fraud Business e-mail Compromise 3rd party loss	The insured works in a profession that handles 3rd party's money in Trust. The insured received an email that looked like instructions from the 3rd party to transfer money to a bank account. The email was fraudulent and they weren't who they said they were. As a result, the insured transferred the money and the 3rd party was unable to stop the bank transfer.	Cyber Event Protection will cover for the insured's Cyber Event response costs to remove the threat and secure the e-mail system. If Cyber Theft coverage is applicable, the direct financial loss the insured's client suffered will be covered as well.
Contingent Business Interruption	An external supplier suffers a CryptoWall malware attack. Their 'Just In Time' manufacturing plant grinds to a halt for three weeks while engineers and IT experts scramble to restore systems and production. As a result of the supplier's Cyber Event, the insured could not source critical components and manufacturing operations were interrupted.	If Contingent Business Interruption cover is applicable, we will pay the insured's impact on business costs arising from an outage at the insured's external suppliers' business.

Disclaimer:

These claims examples related to coverage provided under Emergence's EME CEP002 Cyber Event Protection policy wording.