Claims Examples

emergence

Cyber Event Protection-004 (CEP-004)

Cyber insurance helps business recover after a cyber event. Businesses are increasingly reliant on technology, digital products and third party services to conduct their operations. This further emphasises the need for cyber protection as part of their risk mitigation strategy.

Our Cyber Event Protection insurance provides a broad range of cover:

- Protection against a drop in revenue
- Response costs and support to get the insured back in business
- Public relations / crisis management costs
- Protection against third party liability
- Criminal financial loss including cyber theft, identity-based theft, telephone phreaking and cryptojacking
- Socially engineered theft
- Protection against tangible property damage to the insured's IT

Example	Claim Scenario	Cyber Event Protection Solution
Extortion Attempt	A malicious actor pretending to be tech support gained access to a manufacturing plant'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 covers key response costs including: IT forensics, crisis management and public relations, notification costs, credit and identity monitoring and pursuit costs against the perpetrator. It also covers mandatory data breach notifications, including notice to regulators because of the manufacturer's failure to keep information secure. Defence and settlement costs for third party claims made against the insured are also covered.
Cryptolocker Attack	An employee clicked on a plausible email attachment which unleashed a CryptoLocker virus. This prevented the nursing home from operating their systems.	Cyber Event Protection provides coverage for IT forensic technicians to remove the virus, restore the data and secure the IT systems. Resulting loss to the business from decreased revenue or increased costs is also covered.
Hacking	A retail clothing store operated an E-commerce website which became infected with malicious code. As a result the website showed black screens to customers and staff were unable to access orders in the system.	The policy covers removal of the malware and restoration of the website. The impact of lost revenue and increased costs caused by the attack is also covered.
Tangible Property	A property manager's server suffers heat damage during a cyber attack and is no longer suitable for commercial service.	Optional Tangible Property coverage covers the cost of repair or replacement of the damaged equipment.
Contingent Business Interruption – supplier outage	An external supplier of a bedding manufacturer 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 would pay the bedding manufacturer's impact on business costs arising from an outage at the external suppliers' business.

Claims Examples

emergence

Example	Claim Scenario	Cyber Event Protection Solution
Business Interruption – preventative shutdown	A medical equipment manufacturer was advised by the Computer Emergency Response Team (CERT), which is part of part of the Australian Signals Directorate (ASD), that they had reason to believe that the Insured's system had been breached by a nation state backed threat actor. They instructed the Insured to halt all manufacturing and business. CERT warned the Insured that data exfiltration was likely as well as sabotaging the manufacturing process. The Insured followed the instructions to immediately shutdown down their systems and manufacturing work to assess whether their system had been breached and to also ensure their system was adequately secured.	Cyber Event Protection provides a Preventative Shutdown Allowance which includes the impact on revenue, increased costs to avoid a reduction in revenue and an independent security audit to assess the threat to IT infrastructure.
Contingent Business Interruption – system failure	The Insured operates an accounting practice and utilised a third-party contractor to manage its IT infrastructure. The IT infrastructure unexpectedly became non-operational. This had a significant impact on the Insured's ability to operate. It took the IT contractor seven days to rectify the issue, which was eventually traced back to a combination of human error and equipment failure.	If Contingent Business Interruption cover is applicable, we would pay the impact on business costs arising from the IT system failure.
Identity Theft – stolen identity	A large sporting goods retailer suffered a data breach that led to Personally Identifiable Information (PII) of a number of employees exfiltrated from the system. It was established that the threat actor had stolen the identity of six employees. Luckily, these employees did not suffer a direct financial loss.	In respect of the employees impacted by the loss of PII and stolen identity, Cyber Event Protection provides for credit and identity monitoring costs to the employees for up to 12 months. The Policy also provides identity theft response costs which will support the employees with reporting of the identity theft and re-establishing identity and essential records.
Identity-based theft – loss of personal funds	Ms Jones worked in the sales department of a sporting goods retailer. The Insured suffered a breach to their systems which enabled the threat actor to obtain personal information about Ms Jones, including personal bank account details. The threat actor was able to steal personal funds from Ms Jones bank account.	If Criminal Financial Loss coverage including Identity Based theft is applicable, then the lost personal funds of Ms Jones will be covered under the policy.
Privacy Error	An employee of a medical practice sent an administrative email to its patients advising of altered trading hours over the Christmas period. However, the employee inadvertently attached an excel spreadsheet to the email that provided personal information of some patients. The spreadsheet included patients name, address, Medicare number and a short description of their last visit.	Cyber Event Protection provides Notification costs which includes the cost of notifying the individuals impacted and notifying the Office of the Australian Information Commissioner or other authorities (such as medical authorities). The Policy can also provide identity theft response costs to the individuals impacted by the privacy error.

Criminal Financial Loss Claims Examples

emergence

Example	Claim Scenario	Cyber Event Protection Solution
Socially Engineered Theft 1st Party Loss	An accountant's employee receives a request from a regular supplier's email address for payment of an outstanding invoice. The employee pays the supplier in good faith and in reliance upon the received invoice. As it turns out, the supplier's invoicing system was hacked and the supplier's bank account details were changed to the hacker's account. The paid amount is unrecoverable as a result.	If the accountant's policy includes Optional Cover for Criminal Financial Loss including Socially Engineered Theft, the direct financial loss to the accountant is covered, including investigation costs.
Socially Engineered Theft 1st Party Loss	A medical centre received communications from a fraudster impersonating the ATO requiring urgent payment of outstanding taxes. The medical centre paid the 'outstanding' taxes in good faith having believed the demand was genuine.	If Criminal Financial Loss coverage including Socially Engineered Theft is applicable, the lost funds are covered including investigation costs.
Cyber Theft Business e-mail Compromise	The CFO received a fraudulent email from the CEO, whose e-mail account had been compromised due to a Cyber Event, requesting the transfer of a large sum of money. The email convinced the CFO to transfer money to a third party bank account. Later its determined that 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 forensic investigation of the crime as well as 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.
Telephone Phreaking	A marketing firm's phone system gets hacked. The hacker creates a mailbox to route calls overseas. The unauthorised international calls result in thousands of dollars in call charges.	The policy covers the cost to investigate and remove the threat to the firm's telephone system. Our optional Cyber Theft and Telephone Phreaking Cover pays the direct financial loss to the insured.
Cryptojacking	The insured notices their computers are running slower than usual. Upon further investigation, someone has hacked into their IT infrastructure to utilise the processing power to mine cryptocurrency.	Cyber Event Protection will cover response costs to remove the virus. If Criminal Financial Loss coverage is applicable, the increased bandwidth and electricity costs are also covered.
Cyber Theft	The accounting system of an advertising agency was accessed by a threat actor who altered the bank account details of a supplier. The following day the Insured processed a payment to that supplier, unaware that the bank account details had been altered by the threat actor, resulting in the funds being misappropriated by the fraudulent party.	If Criminal Financial Loss coverage, including Cyber theft is applicable, the lost funds are covered, including investigation costs.

Disclaimer:
These claim examples illustrate the potential scope of coverage provided under Emergence's EME CEP-004 Cyber Event Protection policy wording. Each claim is different and outcomes may vary on a case by case basis depending upon the facts and details of the particular situation.