CYBER EVENT PROTECTION

emergence

claims examples

Cyber insurance helps businesses 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.

Cyber cover includes:

- → 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.

Optional cover includes:

- → Criminal financial loss including cyber theft, identity-based theft, push payment theft, telephone phreaking and cryptojacking.
- → Socially engineered theft.
- → Protection against tangible property damage

Example	Claim scenario	Cyber Event Protection solution
Cyber Extortion (Ransomware)	The insured experienced unexplained server failures. Only when the ACSC warned of an imminent ransomware threat via email, suspicion of a cyber incident was raised. The subsequent investigation uncovered substantial data theft from the file server, persistent unauthorised access, and exploitation of known vulnerabilities spanning months. Multiple state and Commonwealth agencies requested information in response to the incident.	The Incident Response team promptly engaged trusted experts to help respond to the incident. Firstly, a Digital Forensics & Incident Response expert investigated and secured the environment, identified the incident's root cause, and assisted with security recommendations. Legal counsel then advised on legal obligations, reviewed the compromised data, and facilitated notifications and reporting. Crisis Communications experts managed external communications to minimise damage to the reputation. Professional Identity support services aided affected individuals and redirected inquiries for a focused incident recovery. These costs are covered under our Cyber Event Protection policy as Section C Cyber Event Response Costs.
Business Email Compromise (Hacking)	A Microsoft 365 account owned by an insured staff member was compromised, leading to the unauthorised sending of phishing emails to 2,767 recipients. The threat actor also gained access to the insureds SharePoint files, including a document containing usernames and passwords. Additionally, the attacker sent targeted emails to two clients, alerting them of altered bank details, resulting in payments being redirected to the threat actor's account.	A phishing-related account compromise was identified, and legal costs were incurred obtaining advise on legal obligations including reporting the breach. Our Cyber Event Protection policy covered the legal costs, digital forensics and incident response costs under Section C Cyber Event Response Costs. The optional Criminal Financial Loss cover compensated the insured for direct financial losses from altered client payments. The Emergence Incident Response team guided the insured through the process, advising the implementation of a two-step payment approval process whenever changing existing payments details.

CYBER EVENT PROTECTION

emergence

claims examples

Example	Claim scenario	Cyber Event Protection Solution
Socially Engineered Theft	A staff member received an email supposedly from a client, containing updated bank details. Without confirming the changes with the client, the insured unknowingly fell victim to a threat actor who had compromised the client's email. Consequently, a significant payment was issued to the fraudulent bank account, resulting in a substantial financial loss for the insured.	The Emergence Incident Response team promptly advised the insured to report the fraudulent transaction to the bank for potential recovery and recommended checking email systems for compromise. Despite efforts, the funds remained unrecoverable. Under the optional Criminal Financial Loss cover, the insured was compensated for the socially engineered theft, as the electronic transfer led to a direct financial loss covered by the policy.
Business Email Compromise	A medical practice's reception mailbox was breached, and a phishing email was then sent to over 1000 contacts. The email contained a fraudulent link that led to a credential harvester for usernames and passwords. The practice faced a wave of privacy queries. Patients were distressed about the security of their medical and personal information if they had entered their credentials.	The Emergence Incident Response team took immediate action to engage a Digital Forensics expert to investigate and secure the insureds environment. The root cause of the incident was identified, and security recommendations were provided. The digital forensics costs were covered under Section C Cyber Event Response Costs. The investigation revealed the compromise was limited to the reception mailbox and no medical data was impacted. The Emergence Incident Response team drafted communications to reassure clients their medical data was safe.
Cyber Extortion (Ransomware)	The insured learned of an IT system compromise when a user reported login issues. The Managed Service Provider (MSP) discovered a ransom note and subsequently shut down the insureds IT system. Digital forensics confirmed data exfiltration and encryption of the environment. The Insured's practice management software held significant amounts of sensitive personal information.	A number of experts were appointed to assist the insured, with those costs covered under Section C of the policy. Digital Forensics investigated the root cause and secured the IT system. Crisis Communications experts managed media attention and internal communications. Ransom Negotiators engaged with the threat actor, significantly lowering the ransom payment, and ensuring compliance with sanctions checks. Emergence Incident Response team triaged and guided the experts to successfully restoring the practice's IT system.
Business Email Compromise	A medical practice discovered that their email had a been compromised and was used to send out phishing emails to their patients. After the discovery, a password reset was conducted promptly. However, it was unknown how long the attacker had access to the compromised email account, which raised concerns as that account was used by medical staff to share patient information, reports, referrals between clinics, payment information, Medicare details and medical history.	Forensics investigated the incident, discovering a third-party application in their Microsoft environment, which had the ability of copying the entire mailbox. Legal counsel was retained to provide privacy advice, draft notifications to relevant government bodies and individuals and conduct an eDiscovery. The insured received support in issuing notifications along with IDCARE to support affected individuals.

CYBER EVENT PROTECTION

claims examples

Example	Claim scenario	Cyber Event Protection Solution
Cyber Extortion (Ransomware)	The Insured contacted the Emergence hotline after they discovered some of their servers were encrypted by a ransomware demand made by a threat actor. While some IT systems were unaffected, which allowed the insured to remain operational in the short-term, crucial data for long-term operation was inaccessible.	Forensics experts were engaged to understand initial access, the extent of the incident, and actions performed by the threat actor. Legal counsel provided privacy advice and assisted with communications with stakeholders. Ransom negotiators managed the communication with the threat actor. They were able to efficiently communicate and negotiate with the attacker, who provided the decryptor for free and additionally, was no longer seeking ransom payment. All above costs were covered under the policy - Section C - Cyber Event Response Cost.
Business Email Compromise (Hacking)	An international energy and mining company discovered they had a business email compromise. They identified a staff's email was used to run a phishing campaign to approximately 500 recipients. Upon investigation it was identified that the user clicked on a phishing email, compromising their credentials.	We engaged Digital Forensic investigators to investigate the extent of the compromise and actions taken by the threat actor. They determined 6 additional mailboxes had been compromised and 1 mailbox had been exfiltrated. Legal counsel were retained to conduct a review of the data in the mailbox, provide advice on privacy obligations, and draft notifications to affected individuals and the OAIC. All above costs were covered under the policy Section C – Cyber Event Response Costs.

emergence