Cyber Insurance

FTA's cyber policy provides the insured with protection for

Confidentiality, Integrity and Availability

It can also provide additional protection for Claim Preparation costs, Cyber Crime including Social Engineering Fraud, Media, Payment Card Industry (PCI) and Personal Information Violation.

1. **Breach of Confidentiality** (including threatened disclosure)
    a. ***IT forensic investigation costs*** being the cost of IT security experts to confirm the existence or absence of a suspected security breach where it is suspected this will result in a breach of privacy or confidentiality and to establish the breadth of the information that is or could be compromised.
    b. ***Liability to another party*** being both damages and claim costs.
    c. ***Privacy response costs*** including crisis management costs, legal advice on the insured's obligations, costs to notify affected individuals, costs of a call centre to take inbound calls from individuals that have been notified, and costs to redeem an offer to provide credit file monitoring product or an identity monitoring product.
    d. ***Regulatory actions*** including regulatory penalties, regulatory costs due to a regulatory action arising from a breach of privacy.
    e. ***Extortion*** which is extortion loss including an external expert to investigate and response to the extortion threat or to mitigate the extortion threat.
2. **Breach of Integrity of the Insured's system**
    a. ***IT forensic investigation costs*** being the cost of IT security experts to confirm the existence or absence of a suspected security breach where it is suspected this will result in the encryption, damage or destruction of the insured's data assets (including 3rd party data assets on the insured's systems), the transmission of malicious code, the unauthorised use of the insured's systems for the purpose of participating in a denial of service attack.
    b. ***Liability to another party*** damages and claim costs due to the Insured's failure to prevent a security breach that has resulted in transmission of a malicious code, encryption, erasure or destruction of a 3rd party's assets on the insured's systems, the unauthorised use of the insured's systems for the purpose of participating in a denial of service attack.
    c. ***Data Restoration costs*** being costs for the recovery or restoration of the insured's data assets that have been encrypted, damaged or destroyed due to accidental damage, operational error or a security breach.
    d. ***Business interruption loss*** due to the insured being unable to reliably use its data assets due to an operational error or security breach.
    e. ***Extortion*** which is extortion loss as a result of a credible threat to destroy or encrypt the insured's data assets due to a security breach.

3. **Availability of the insured's system to 3rd parties**
    a. ***IT forensic investigation costs*** being the cost of IT security experts to confirm the existence or absence of a suspected security breach where it is suspected this will result in a denial of authorised access to the insured's computer systems by an authorised 3rd party or impairment (or threat of impairment) of the insured's computer systems.
    b. ***Liability to another party*** damages and claim costs due to the insured's failure to prevent a security breach that results in the prevention of authorised access to the insured's computer systems by an authorised party.
    c. ***Business interruption loss*** due to the availability of the insureds computer systems being impaired due to an operational error, denial of service attack or a security breach.
    d. ***Extortion*** which is extortion loss due to a credible threat to impair the availability of the insured's computer system as a consequence of a security breach or denial of service attack.

Additional Optional Protections

- **Claim Preparation costs $50,000** being the costs of an accountant to prepare a submission for the purposes of evidencing any covered business interruption loss.
- **Reputational Damage** loss of nett profit from impairment of your brand or reputation that has directly resulted from media reporting of a breach of privacy or a breach of confidentiality
- **Cyber Crime and Social Engineering Fraud** covers loss from having transferred funds or property in reliance on verified instructions where access to the insured's computer systems has been gained as a result of a security breach.
- **Media** which covers damages as a result of defamation, violation of a right to privacy, infringement of intellectual property or plagiarism.
- **Payment Card Industry (PCI)** covers PCI fines, PCI assessments and related PCI claims costs for a payment card breach as a consequence of the insured's failure to comply with published Payment Card Industry Data Security Standards (PCI DSS).
- **Personal information Violation** covers damages and claim costs as a result of unauthorised collection or use of personally identifiable information in violation of any law or the insured's privacy policy.

Underwriting

Contact us: 02 9003 1660 **quotes@FTAinsurance.com.au**

Lewis Patton
National Underwriter &
Cyber Liability Manager
D – 02 9003 1662
M – 0414 048 144
lewis@FTAinsurance.com.au

Incident response service

FTA's incident response service is proudly provided by

CLYDE&CO

Cyber incident response hotline: 02 9210 4464

Cyber incident response email: cyberbreach@clydeco.com

Tried and tested methodology - Having dealt with over 200 data breach and cyber related incidents in Australia in recent times, Clyde & Co has developed and refined its methodology to manage the threat and mitigate the risk, with a view to reducing the resulting damage. Clyde & Co have expansive processes and technologies that sit behind its incident response service offering. Clyde & Co's unique approach to the management of incidents provides clients with peace of mind that the incident is managed proactively with loss mitigation front of mind. Rather than detail the processes (which Clyde & Co can should you need further detail), the below summary is provided.

Effective incident management – Clyde & Co's first class incident response team are experts in effectively managing all incident types. Clyde & Co understand how to engage with an organisation and the key decision makers to ensure your insured feel supported throughout the lifecycle, including incident debriefs.

Bespoke experience – Clyde & Co have tailored a number of breach response processes to meet the particular needs and work flows of our clients, including FTA Insurance.

Sector focus – Clyde & Co triage process (including scripts) are both incident type and sector focused. Your insureds will experience an incident response solution that fits their business needs.

Incident Response Partners

IT Forensics partners include Content Security, Klein & Co, Deloitte, KPMG, EY, Mandiant, Grant Thornton, McGrathNicol, FTI Consulting, Schatz Forensics, Hivint, Sententia, IBM and Insane Technologies

Cyber security / technology / risk consulting partners Contextis, Control Risks Crowdstrike and Kroll

Public Relations partners Fleishman Hilliard, Fowlstone Communications, GRA Cosway, Hill & Knowlton and Porter Novelli

Notification services / Credit Monitoring partners ID Care (call centre / ID restoration), Stellar (call centre), Well Done (call centre), Bluestar Group (direct mail / email / SMS), LinkDigiCom (direct mail/ email/SMS), Mmw3 Degrees (direct mail/email/SMS) and Epiq (notification / credit monitoring)

Loss Quantification partners Korda Mentha, Matson, Driscoll & Damico Pty Ltd, RGL Forensics and JLT Forensics