CHUBB®

MasterPackage for Technology Companies

A Comprehensive Solution For Technology Companies

The Insured is a medical clinic software developer delivering cloud-based SaaS (software as a service) model to clients, including doctors, hospitals and clinics.

The Insured's system was affected by malware, allowing unauthorized access to their database infrastructure. The database held sensitive client data for clients in Australia, Singapore, the UK and the US.

The Insured's forensic investigation concluded that data was accessed and clients' patient personal information was extracted and later discovered that it was published on the Internet.

The hacker attempted to extort the Insured, threatening to release the data, but the Insured rejected the extortion demand.

Clients made claims seeking damages for:

- Breach of contract for failing to protect data
- Loss of profit, additional costs of working from their business interruption
- Forensic investigation costs
- Regulatory reporting costs
- Regulatory fines
- Clients' patients seek damages for breach of privacy.

Many of the Insured's clients stopped using the software. Some of its clients also notified their own cyber insurers of the data breach.

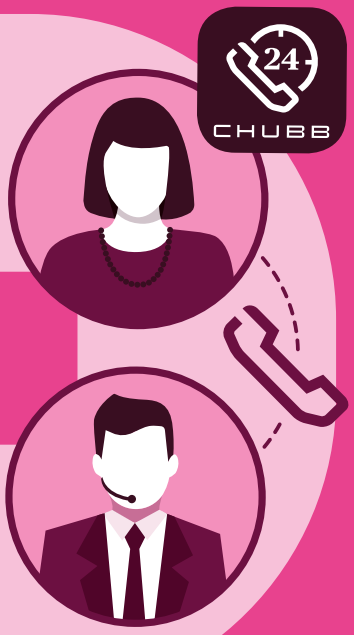
MasterPackage for Technology Companies is a total solution providing services and coverage that will respond to this incident, including first party coverage for remediation expenses, third party liability coverage and access to our incident response vendors.

The Chubb Incident Response Platform is available 24/7/365. It provides access to the Chubb Cyber Incident Response Centre and our Cyber Incident Response Team and offers a holistic approach to managing cyber events.

GET IT ON Google Play

Download on the App Store

The Chubb Incident Response Manager in consultation with the Insured conducted initial investigations into the cause of the incident and developed an incident response plan of action.



A legal adviser was engaged to assist with complying with notification provisions of privacy regulations.

An extortion consultant was engaged to handle the negotiation with the hacker.

A public relations rm was engaged to help protect the reputation of the Insured.

An IT forensics firm was engaged to investigate the extent systems have been compromised by the malware.

Technology Professional Indemnity provides protection for:

- Claims Expenses to investigate and defend the Insured against the claims being made by the doctors, the clinics and the patients.
- To mitigate a potential claim, the company will pay amounts that the Insured has invoiced to a customer but is unable to collect due to an incident which would lead to a potential claim if the Insured pursued the outstanding amounts.

Technology Professional Indemnity provides protection for:

- Client business interruption claims, their loss of profit, additional costs of working, forensic investigation costs, regulatory reporting costs and regulatory fines incurred due to defects in the Insured's services and its failure to perform their services in accordance with the SaaS agreement.
- Liability to clients arising out of the failure to manage and store corporate information and personal data is covered under Privacy and Network Security Liability.

Technology Professional Indemnity provides protection for:

- Privacy and Network Security Liability resulting from the liability the Insured has to patients arising from the failure to manage and store their personal data.

Cyber section provides protection for:

- The Insured's Incident Response Expenses and Cyber Extortion Expenses incurred by the vendors appointed by the Incident Response Manager.
- Data and System Recovery Costs for the cost to repair and restore the medical clinic software application and database to an equivalent condition before the malware attack.

www.chubb.com

Chubb. Insured.™

uk7980 - 03/21