CHUBB®

PremierTech2

# Cyber incident case study:

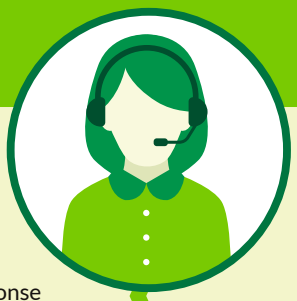
## Ransomware attack

The Insured is a software company with an annual revenue of **$15 million.**

### Day of Incident

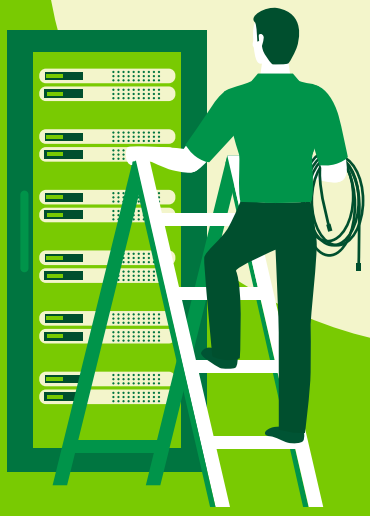
During the weekend, a malicious file infected the company's servers and all files including historic and current project data were affected.

With the servers down, the Insured was unable to fulfil their clients' orders. Business interruption loss was estimated to cost over **$125,000** a day. The hacker demanded a ransom to decrypt each server, with the ransom amount increasing daily if not met.



The Insured reported the incident to Chubb and spoke to the Incident Response Manager on the same day. An IT forensics firm was deployed immediately.

Chubb's Incident Response Team assisted the Insured with a mitigation strategy by identifying less business critical servers that could be restored from backups, and negotiating the ransom amount to release business critical servers.



### 3 Days from Incident

The response team removed the ransomware from the affected servers, allowing the company to operate at 70% of typical capacity. The response team also engaged a crisis management firm to assist with client communications.

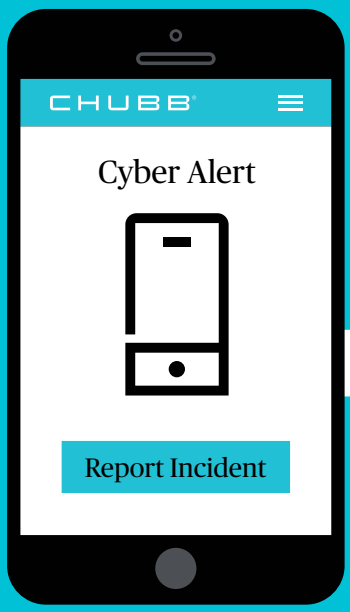
Legal advisors assisted the Insured with the filing of a formal criminal complaint as well as other regulatory documentations.

### 10 Days from Incident

100% of operations restored.

The IT Forensics provided an incident report to the Insured, with recommendations to improve cyber security and prevent future incidents.

This cyber incident was reported through Chubb's 24/7/365 Cyber Alert mobile application which can be downloaded straight from the App Store (for iPhones) or from the Google Play Store (for Android devices) – just search 'Chubb Alert'. The following stakeholders were activated to provide a holistic response to the Insured's cyber incident.




**Estimated Cost**
**$100,000**

Incident Response Manager

Legal Advice

IT Forensics

Crisis Management Firm

Forensic Accounting

## Coverage

- The Incident Response and Cyber Extortion insuring clauses were initially triggered in response to the cyber incident.
- Additionally, the incident response process triggered several other insuring agreements.

First Party

### Incident Response

Costs to mitigate any cyber incident:

- IT Forensics
- Legal Advice
- Notification
- Fraud Restoration
- Call Centre
- Public Relations

### Business Interruption

Covers loss of net profit and continuing operating and payroll expenses.

> Triggered by Business Interruption Incident.

### Data and System Recovery

Increased cost of work and other costs to recover data, repair or restore software, identity and remove malware, and to recover business operations.

> Triggered by Business Interruption Incident.

### Technology Professional Liability

Defence and damages for claims arising from:

- Defect or deficiency in the insured's service during the ransomware attack.
- Liability to customers of data that the insured manages on their behalf.

### Privacy & Network Security Liability

Defence and damages for claims arising from:

- Duty to maintain confidentiality of your own personal data.
- Introduction of malicious code into third party's systems.

Third Party

### Cyber Extortion

Covers a cyber extortion payment and the cost to hire a crisis negotiation specialist.

> Triggered by Cyber Extortion.



Chubb. Insured.℠