

MasterPackage for Technology Companies

Cyber incident case study: Ransomware attack





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.





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





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 if payment was not made within 2 days.



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.



Coverage

First Party

The Incident Response and Cyber Extortion insuring clauses initially triggered in response to the cyber incident; however, the incident response process impacted several other insuring agreements.



Incident Response

Costs to mitigate any cyber incident:

- Incident Response Manager IT Forensics Fraud Restoration

- Call Centre • Public Relations



Business Interruption

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, identify and remove malware, and to recover business operations.

Interruption Incident.



Reputational Injury & Media Act

Defence and damages for claims arising from improper online media activity.

Privacy & Network Security Liability Defence and damages for claims arising from:

- · Duty to maintain confidentiality of personal or corporate information
- Duty to maintain a secure network for third parties



Cyber Extortion

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

> Triggered by Cyber Extortion.