CYBER COVERAGE PREVENTS FINANCIAL DISASTER FROM SYSTEM LOCK-OUT

CASE IN POINT: Ransomware attack on law firm
COMPROMISED: Ability to conduct business
DEMANDED: $30,000 ransom

THE CYBER ATTACK
A law firm’s IT department discovered a system lock-out, confirming a data breach. A cyber criminal then demanded a $30,000 ransom in Bitcoin in exchange for the encryption key to restore system access.

THE IMPACT TO THE LAW FIRM
Thirty minutes after the client notified Corporate Synergies of the attack, a senior claims counsel representative from the insurance company was on the phone with the law firm’s executive liaison and the IT department.

Additional cyber experts, including forensic investigators, immediately began to resolve the ransomware incident by:
- Examining the firm’s computer system and identifying the vulnerability that had opened the back door to the cyber criminal.
- Arranging for the ransom payment in Bitcoin, the method demanded by the hacker.

Within 48 hours, the insurer’s cyber experts resolved the system vulnerability that led to the attack. Experts also paid the ransom in Bitcoin on behalf of the client. Following the payment, the hacker delivered the encryption key and the firm’s access to its records and data was restored.

Last year, ransomware attacks generated $1 B for cyber criminals. Targeted attacks on businesses are becoming more frequent with phishing email attachments as the No. 1 delivery vehicle for ransomware.

Source: Barkly, 2017 Ransomware Trends and Forecasts

1Ponemon Cost of Data Breach Study: United States

CYBER INSURANCE COVERAGE

Five months prior to the ransomware attack, Corporate Synergies’ P&C Practice experts conducted a review of the law firm’s coverages and recommended a First- and Third-party Cyber Insurance policy.

First-Party Cyber Insurance
Protects the insured if they are breached directly by providing resources to manage:
- Business Interruption
- Data loss/destruction
- Computer fraud
- Post-breach forensic investigation
- Public relations
- Cyber extortion
- Notification costs

Third-Party Cyber Insurance
Protects the insured if their vendors/third-party administrators are breached by providing resources to manage:
- Business Interruption
- Data loss/destruction
- Post-breach forensic investigation
- Public relations
- Notification costs
- Legal defense settlements, damages, and judgments
- Defense costs related to claims by state regulators
- Fines and penalties
Ransomware Attack Defined

Ransomware is a type of malicious software that threatens to publish the victim’s data or perpetually block access to it unless a ransom is paid. Ransomware lures users into clicking on an attachment that locks up systems.

THE BOTTOM LINE

It takes an average of 46 days to resolve a cyber attack at a cost of $21,155 per day, or a total cost of $973,130.¹ The law firm’s Cyber Insurance policy reimbursed the $50,000 claim for all costs associated with the attack. There was no financial impact to the firm beyond the ransom payment² and the initial $3,000 annual policy.

Cyber attacks are lurking disasters. It’s not a matter of if a professional services organization will be hit with an attack, but when.

In the case of our client, their Cyber Insurance coverage prevented a protracted business interruption and the loss of hundreds of thousands of dollars to restore system access.

¹ Ponemon, “Cost of Data Breach Study: United States”
² Ransom payments are not typically covered by Cyber Insurance

Synergies360™

Corporate Synergies takes a full view of the insurance landscape, studies it from every angle, pursues innovation where none exists, and transforms this deeper understanding into actionable strategies to protect our clients and their participants. We call our approach Synergies360.

For more information visit corpsyn.com or call 877.426.7779