

CYBER RISK PROTECTION REALLY PAYS: 8 REAL-LIFE SCENARIOS PROVE IT.

Technology can open up companies to liabilities they may never have known were possible. Different aspects of certain claims or incidents have the potential to trigger more than one policy. The ability to coordinate a multiline insurance and risk management program, including cyber risk insurance, can be critical to your clients.

One innocent mistake by an employee, such as opening an electronic document embedded with malicious software, can result in exposing confidential personal or corporate information. In addition, determined cyber criminals can hack, steal data, collect ransoms and leave destruction in their path resulting in potential liability costs and lost revenues that can cripple a company financially.

SCENARIO 1: REMOTE THEFT AT THE CHECK-OUT

Type of insured: Small business providing cash registers and point-of-sale terminals to retailers

What happened: Criminals remotely accessed the sales terminals of the company's largest client (a restaurant chain) by using the company's employee credentials through a leaky software application.

What followed:

- The restaurant chain had to notify its customers of the breach
- The company is facing an indemnification claim from the client

What could help: Data Privacy and Network Security Liability, Privacy Regulatory Matters

SCENARIO 2: RANSOMWARE ATTACK

Type of insured: Regional accounting firm

What happened: A ransomware attack blocked all access to the firm's computer system, while deleting files. After the firm paid the ransom, it took several days to restore its applications and recover deleted files from its backup.

What followed:

- The firm was unable to meet tax filing deadlines
- Brand and reputation damage

What could help: Incident Response Expenses, Cyber Extortion Loss, Network Restoration Expenses, Business Interruption

SCENARIO 3: WHITE HAT HACKER

Type of insured: Small company with an online sales platform

What happened: A “white hat hacker” alerted the company to a back door in its system. He then blackmailed the company, threatening to broadcast the breach to its customers unless the company paid him two bitcoins for his “service.”

What followed:

- A forensics analysis confirmed that the sales platform was severely compromised
- To prevent future incursions, the data had to be migrated to a new platform

What could help: Incident Response Expenses, Cyber Extortion Loss, Network Restoration Expenses

SCENARIO 4: HR IMPOSTER

Type of insured: Construction company

What happened: A thief purporting to be the managing partner of the firm sent the HR payroll manager an email, requesting W2 forms of all 150 employees via PDF. Too late, the payroll manager realized the email address was spoofed.

What followed:

The construction company had to notify and provide credit and identity monitoring services to its employees in the wake of the incident.

What could help: Incident Response Expenses

SCENARIO 5: FACEBOOK INVASION

Type of insured: Company that provides technicians to a laptop manufacturer’s repair center

What happened: While a young woman’s laptop was in the custody of technicians at the center, her Facebook account was hacked and several sexually explicit photos were posted to it.

What followed:

- The young woman negotiated a quick, pre-litigation multi-million dollar settlement with the laptop manufacturer, who avoided publication of the incident
- The manufacturer, in turn, demanded that the staffing services company indemnify it for the privacy breach and publication

What could help: Data Privacy and Network Security Liability, Media Liability

SCENARIO 6: CARPETBAGGERS

Type of insured: Carpet factory

What happened: Unknowingly, an employee clicked on an email attachment laced with cryptowall malware. This led to a hack that paralyzed the company’s access to data and production files, with a demand for ransom. The company paid the ransom the next day.

What followed:

- Production was halted and costs racked up
- An external consultant was unable to clean up the network
- Without up-to-date backups, the company lost data
- Deadlines were missed
- Significant damage to brand and reputation

What could help: Data Privacy and Network Security Liability, Incident Response Expenses, Cyber Extortion Loss, Network Restoration Expenses, Business Interruption

SCENARIO 7: DEEP FREEZE

Type of insured: Online travel reservation company

What happened: During some routine system upgrades, human error in coding caused the entire network to freeze. Customers couldn't access the reservations site for 12+ hours. It took several days until the network was fully operational.

What followed:

- Lost revenue and harm to the brand
- Customers went elsewhere to book their travel reservations

What could help: System Failure for Administrative Error

SCENARIO 8: DOUBLE TROUBLE

Type of insured: Bank

What happened: To divert attention away from a hack into the bank's network, hackers began a DDoS attack on a bank's website. This shut down the bank's online banking operations for three days. Hackers also accessed customers' social security numbers, which ended up on the dark web.

What followed:

- The insured had to notify and provide identity and credit monitoring to its customers
- The insured paid the ransom demand
- A class-action lawsuit was filed by impacted customers
- Regulators launched investigations
- The insured experienced lost revenue and harm to the brand

What could help: Data Privacy and Network Security Liability, Privacy Regulatory Matters, Incident Response Expenses, Cyber Extortion Loss, Network Restoration Expenses, Business Interruption

FIGHT BACK. Visit TheHartford.com/cyber today.



Business Insurance
Employee Benefits
Auto
Home

The scenarios summarized herein are offered only as examples. Coverage depends on the actual facts of each case and the terms, conditions, and exclusions of the issued policy. Please refer to the issued policy to determine all terms, conditions and exclusions of coverage. Coverage is provided by the property and casualty companies of The Hartford Financial Services Group, Inc. and may not be available to all insureds in all states. Hartford Financial Products is an underwriting unit of The Hartford. All information and representations herein are as of November 2024.

The Hartford® is The Hartford Financial Services Group, Inc. and its subsidiaries, including Hartford Fire Insurance Company. Its headquarters is in Hartford, CT.

24-GS-2700651 © November 2024 The Hartford