CYBER LIABILITY PROTECTION REALLY PAYS: 10 REAL-LIFE SCENARIOS PROVE IT.

Technology can open up companies to liabilities they may never have known were possible.

One innocent mistake by an employee 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 and costs that can cripple a company financially.

That's why it really pays to have a solid wall of defense in place with a cyber insurance policy you can rely on. Take a look at the scenarios that follow to see how The Hartford's CyberChoice First Response can help companies prevail against cyber threats.

SCENARIO 1: A 6-MONTH HACK

Type of insured: Large retailer

What happened: Hackers gained access to the company's network through social engineering emails. Over 900 of its locations were hacked. By the time the company was alerted by a security blogger, six months had passed and as many as two million customers were affected.

What followed:
- Several class-action lawsuits were filed against the company
- States' attorney generals offices opened investigations
- Affected credit card companies issued PCI fines

What could help: Data Privacy and Network Security Liability, Privacy Regulatory Matters, Incident Response Expenses, Network Restoration Expenses

SCENARIO 2: 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

continued

THE HARTFORD

SCENARIO 3: 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 4: 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 5: HR IMPOSTER

Type of insured: Law firm

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 law firm 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 6: 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 7: 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 8: PRIVACY BREACH

Type of insured: Healthcare provider

What happened: The company sent out a flyer to HIV-positive patients requesting their participation in a research project. The HIV-status of some recipients showed through the glassine envelope. One recipient alleged that this led to being evicted from her apartment when her partner saw the divulged diagnosis.

What followed: A class-action lawsuit was filed

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

SCENARIO 9: 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 10: 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/cyberchoice** today.

Business Insurance
Employee Benefits
Auto
Home