THINK YOU DON'T NEED CYBER INSURANCE IN RETAIL?

CHECK OUT THESE CYBER CLAIMS SCENARIOS

1

Card Skimmers

Identity thieves used card skimmers at a gas station to steal bank account numbers with PIN codes from 550 customers. The thieves then created false debit cards, using the stolen information at ATMs to drain funds from client accounts.

Total Cost: $19,250 under Data Breach Response Expenses (for Notification to Affected Individuals and Services to Affected Individuals)

2

Ransomeware Attack

When ransomware infected servers at a chain of gas stations and convenience stores, over 200 devices at 16 locations were impacted. However, because the insured's IT Director had read the cyber insurance company's advisories on what to do if his system was infected by ransomware, he knew what to do. Rather than pay the ransom demand of $250,000, he opted to wipe the devices, reinstall software and restore data from recent backups. Because the insured had backups that were not affected by the infection, his business was only interrupted for a short time. The insured paid the following costs and was reimbursed by cyber policy, less its deductible.

Total Cost: $89,924 under Data Breach Response Expenses (for Legal Review: $14,926 and Forensic IT Review: $25,000) + Computer Attack (for System Restoration: $19,178, Data Restoration: $30,307 and Loss of Business: $513)

3

Keylogger Corruption

A keylogger originating from the retailer's host captured customer credit card data. An online equipment retailer's server was breached by a keylogger, which captures information typed into the computer. This occurred three times over the course of several months and, with each new breach, customers' credit card numbers were captured. The retailer's server was also corrupted each time and needed to be fully replaced. Finally, IT forensics found the keylogger originated from the retailer's hosting provider but by then 16,000 credit cards had been exposed. Three separate notifications were sent to affected individuals, one for each breach. In total, 315,500 people and 31 attorney generals had to be alerted, all at the retailer's expense. The retailer also paid a high price to restore its data and systems and suffered greatly from loss of business and a damaged reputation.

Total Cost: $207,500 under Computer Attack (System Restoration, Data Restoration and Loss of Business) + Data Breach Response Expenses (for Forensic IT Review, Notification to Affected Individuals and Reputational Harm)

More Scenarios >

4

Security Breach

A retailer's eCommerce provider suffered a security breach, exposing thousands of credit cards. When an eCommerce vendor experienced a data breach, all its clients, including this online equipment retailer and the retailer's clients, were put at risk. Thousands of credit card numbers were exposed and, while the eCommerce provider was at fault, the breach of customer data—and trust—negatively impacted the retailer's business. Fortunately, the retailer's contract with the eCommerce provider included data breach response. So, the costs to notify affected individuals and provide services to address potential fraud were paid by the eCommerce provider. Without this contract provision, the retailer would have been stuck with these expenses. Still, the retailer reviewed its potential legal obligations for which it incurred legal expenses.

Total Cost: $5,000 under Data Breach Response Expenses (for Legal Review)

5

Cyber Extortion

The employee of a retailer received an email appearing to come from her company's owner, asking for employee information. She replied asking why he needed it but gave him the information. Later in the day, the insured felt that something wasn't right, so she reached out to the owner and asked if he emailed her, and he responded in the negative. She had provided information to an unknown third party that may have included the Personally Identifiable Information of the insured's 150 employees.

Total Cost: $6,020 under Data Breach Response Expenses (for Legal Review: $4,774, Notification to Affected Individuals $286, and Services to Affected Individuals: $960)

6

Fraudulent Website Charges

A retailer's bank notified the insured after discovering fraudulent credit card transactions on their website. The Insured investigated and found that their website had been affected. The insured's bank could not assist in the notification of the affected individuals, but the this insured carried Cyber Suite insurance; breach counsel was offered to the insured and those expenses as well as the notification to the affected individuals was covered under this endorsement.

Total Cost: $17,251 under Data Breach Response Expenses (for Legal Review: $5,000, Notification to Affected Individuals: $11,234 and Services to Affected Individuals/credit monitoring & case management: $1,017)

7

Infected Server

The insured furniture store had a trojan downloaded to one of their workstations which then infected the server. The insured immediately contacted their IT company to mitigate the issue. The infected machine was wiped clean, and the IT firm restored the server from their backup. The only loss incurred was for their IT company to assist with the remediation and recovery of the network from backups.

Total Cost: $5,650 under Computer Attack (for System Restoration)

8

Litigation

A small online retailer had their privacy policy listed on their website. Even though the small business never had a security incident or data breach, one of their savvy customers who was also a lawyer sued the retailer claiming that their treatment of his personal information violated the retailer's own privacy policy.

Total Cost: $32,360 under Privacy Incident Liability (for defense and settlement, after deductible)