Cyber Exposure: What's the Real Cost?

Real Claims Examples

YETTER INSURANCE

Cyber Exposure: What's the Real Cost?

Cyber security has now become a necessity for every business that uses technology. Nearly every business is at risk of potential cyber attacks. Cyber threats constantly evolve and adapt, making it difficult to both identify and block them. Many business owners don't understand the extent of their own cyber exposure and the devastating costs that these attacks bring. CNBC reported that the average cost of a cyber attack is now $200,000. With the damages of cyber attacks rising, many small businesses are forced to close if they don't have the proper coverage.

So why would any business owner choose not to protect themselves against cyber risks? Sometimes, they simply don't realize they're at risk. Or, they may severely underestimate the damages associated with these attacks.

Cyber Claim Examples

Taking a look at examples of cyber exposures can help demonstrate the damages associated with a cyber attack and who could potentially be at risk. As you'll see, a wide variety of industries are susceptible to cyber events or data breaches.

Here's how types of cyber insurance coverage can protect your clients.

So why would any business owner choose not to protect themselves against cyber risks? Sometimes, they simply don't realize they're at risk. Or, they may severely underestimate the damages associated with these attacks.

1) Healthcare

A private healthcare clinic was the victim of a cyber attack in which patient information was stolen from their computer system. The hackers threatened to post the data publicly unless they received a ransom payment of $13,220 in Bitcoin. They contacted their cyber insurers who helped the healthcare clinic's IT team immediately fix the vulnerability. A local IT forensics specialist began verifying the hacker's claim and was able to confirm that data related to 3,000 patients had been compromised. However, this was data related to names and addresses only.

Ultimately, it was decided that they would not pay the ransom. Instead, their insurer connected the healthcare clinic with a crisis communications consultant who helped them notify all affected parties. They did not hear from the hackers again.

The cost of the IT forensics team and the crisis communications company were both covered under their cyber liability insurance policy, less their deductible.

2) Retail

An online retailer utilized a data center as the host of its company website. When the data center suffered a cyber attack in which an internet of things device was breached, their network failed and the retailer's entire website was inaccessible.

They contacted their cyber insurer, who provided IT services to get their website back up and running in six hours by subcontracting with an external service provider. During those six hours, they lost nearly $100,000 in sales and revenue.

Ultimately, with the costs of recovering the website, lost revenue, and incident response expenses (IT forensics, firm, legal consultation fees, and incident response manager fees) the total cost of the cyber attack was $144,000. Without a cyber policy, the retailer would have faced these expenses out of pocket.

3) Manufacturing

An employee of a car components manufacturing company clicked on a malicious link in a ransomware email and the company's service was infected with malware, encrypting all data. The hackers demanded $13,040 in Bitcoin within 48 hours in order to release the encryption key.

The manufacturing company contacted their cyber insurer who enlisted an IT forensics team to review the threat. Ultimately, they decided not to pay the ransomware demand. The costs of their incident response and the data recovery cost a total of $60,000. Their IT forensics team assigned by their insurer helped lead them through the most prudent course of action when faced with a ransom demand.

4) Food Service

A restaurant suffered a ransomware attack, which affected their entire server. They were unable to utilize their registers, effectively forcing them to shut down.

They contacted their insurer who, after exhausting all options, helped them determine that they would have to pay the ransom. Their insurer covered the costs of the ransom demand, the costs of the IT team's work on applying the decryption key and ensuring that all systems were back and running appropriately. They also enlisted a breach coach to determine if any personally identifiable information had been compromised, along with the revenue lost under business interruption. Had the restaurant not have had a cyber policy, they would have been out of pocket $20,000.

5) Professional Services

A financial controller of a law firm received a call from the firm's bank advising that there had been some suspicious wire transfers in the firm's account. The caller requested the firm's password and pin code to freeze the account and protect the remaining funds. The financial controller provided him with the requested information.

The next day, the financial controller contacted the bank and learned that they had no record of their prior conversation. TThey advised that $118,830 had been wire transferred to a number of overseas accounts, all of which were too late to recall. As this transaction had been authorized by the financial controller, there was nothing the bank could do.

As the firm had a cyber liability policy with cybercrime coverage with social engineering, they were able to recover the stolen funds, less their policy deductible.

6) Communications

A public relations firm noticed an issue with their emails. After their regular IT contractor investigated and realized there was likely malicious activity, they contacted their insurer who enlisted an IT forensics team. It was confirmed that they were the victim of a cyber attack in which their system was infected with cryptojacking malware, which mines for currency. The forensics team was also able to determine that the hackers had likely compromised personally identifiable information in their system.

The forensics team removed the malware and corrected the vulnerability in its system to ensure network security. Their insurer then hired legal counsel to assist the public relations firm with their notification obligations for all parties affected by the data loss. The total cost of the claim between IT forensics, legal and notification costs was ultimately $50,000.

Get Cyber, Get Protected

As you can see, cyber security threats are a serious concern for organizations in nearly every industry. As business owners, it’s important that you act now and get your organization the protection it needs to survive. As cyber attacks grow more serious every day, minimize your exposure with a cyber policy.

Contact us to get started today!