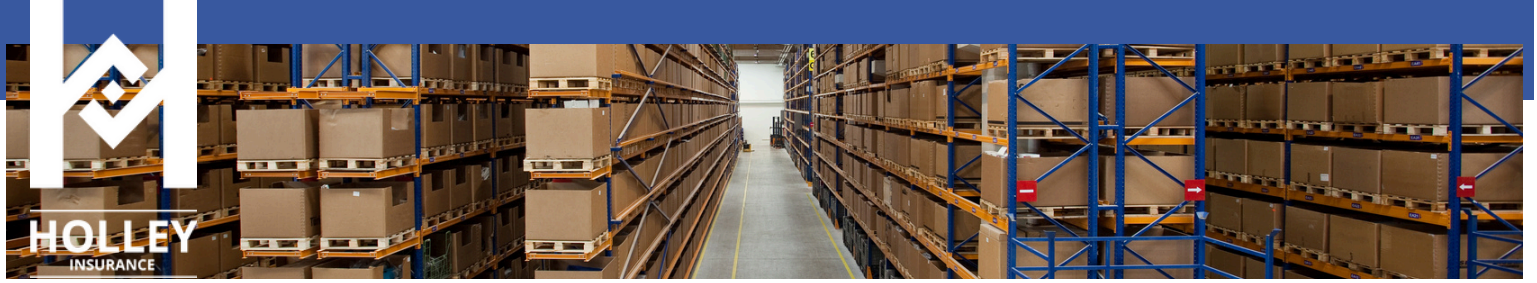

THINK YOU DON'T NEED CYBER INSURANCE IN MANUFACTURING?

CHECK OUT THESE CYBER CLAIMS SCENARIOS

1

Phising Email

The metal manufacturing facility's computer systems were attacked by ransomware that gained access to the system through a phishing email. The ransomware encrypted the data filed and demanded a ransom of 60 Bitcoin ($240K) for decryption. The insured did not pay the ransom. Four months of data had to be recreated by temporary employees. A total of 10 virtual servers, 5 physical servers and 50 workstations were affected. dividuals and regulators and credit monitoring as well as identity recovery case management.

Total Cost: $47,139 under Computer Attack (for Data Restoration, System Restoration and Loss of Business)

2

Data Encryption

A hacker gained access to the manufacturing office insured's computer system via a desktop and got administrative privileges in order to encrypt the insured's data. Proprietary data was lost. IT forensics showed the event occurred in less than two hours. The hacker was able to delete the external back up associated with the server. The entire facility was taken offline while a remote scan was performed. Affected machines had their hardware replaced and backups were restored from a remote site and data had to be recreated.

Total Cost: $41,938 under Computer Attack (for Data Re-Creation and Loss of Business due to the computer attack)

3

Ransomware Attack

A ransomware attack at a machine parts and components manufacturer seized the manufacturer's system and a payment was demanded for release. Employees and vendors are the biggest cyber security weakness for small and mid-sized businesses. In this case, no remote access was detected so it is believed that an employee inadvertently downloaded the ransomware virus while browsing the web. Their lack of security awareness and unsafe online habits opened the door to a ransom demand. The attack brought the manufacturer's system and operations down, halting production. No ransom was paid, but the attack was still costly. An IT provider had to rebuild two servers and five workstations from scratch, which included reloading the operating system and reinstalling all software and other functions.

Total Cost: $22,000 under Computer Attack (for Data Restoration, Data Re-Creation, System Restoration and Loss of Business). Ransom not paid.

More Scenarios >

4

Server Corruption

The owner of a wine and oak barrel manufacturer was having computer issues and hired an external IT consultant to assist. One morning, the insured noticed the computer was glitching, so he attempted to reboot the computer. When the computer restarted, a ransomware message showed up the screen. The insured called the IT consultant, and the ransomware was identified. The IT consultant was able to determine that the server was impacted and advised the insured to shut down all company workstations, including warehouse, office and remote employees. After an investigation, it was determined that only the servers had been impacted and the workstations were not. The insured was referred to a notification legal expert to determine if the insured needed to notify any affected 4 individuals. Through the claims process, they were also able to work with an IT service provider to get the decryption key for the insured.

Total Cost: $9,197 under Computer Attack (for System Restoration: $405) + Cyber Extortion (for negotiator/investigator: $2,710 and extortion payment: $3,000) + Data Breach Response Expenses (for Legal Review: $3,082)

5

Server Encryption

The insured, a manufacturer, discovered that their main server was encrypted with ransomware. The insured identified that no other workstations or servers, other than the main server C-Drive, had been affected. The C-Drive stored the insured's applications which ran to operate the business. The insured was unsure how the ransomware got onto the drive, but it was believed that someone clicked on a malicious pop up. There was no personal information stored on the affected server and the backup files were encrypted. The insured utilized the services of an approved vendor to assist the insured. The ransomware was successfully paid, and the decryption tool was able to decrypt the data. The computer attack was discovered during the policy period and was reported within 60 days of discovery.

Total Cost: $8,810 under Cyber Extortion (for extortion payment: $5,000 + negotiator/investigator: $3,810)

6

System Encryption

The insured, a manufacturer, discovered that his internet service was not working over a weekend and called his IT firm. He discovered a few days later that all his systems were encrypted and received a ransom note. The insured immediately determined they would not pay the ransom. The first attack was on the off-site backups. The insured only had a backup from QuickBooks on his desktop, where personally identifying information for their employees (SSNs, etc.) was stored and password protected. Once claims reviewed the situation, it was determined that the ransom would not be paid; however, breach counsel was engaged, and 154 notifications were sent to affected individuals.

Total Cost: $22,965 under Data Breach Response Expenses (for Legal Review: $10,679 and Notification to Affected Individuals: $797) + Computer Attack (for System Restoration: $5,295 and Data Recreation: $1,244) + Cyber Extortion (for negotiator/investigator: $4,950)

7

Stolen Credentials

A cyber criminal used stolen credentials to infiltrate a machine shop's server and encrypted files with a ransomware virus. A ransom demand of $50,000 in Bitcoin was made. The business owner was introduced to a ransomware specialist and an attorney specializing in cyber and privacy incidents. The insured's team negotiated the ransom down by half, and successfully obtained the decryption keys. A digital forensics investigator and systems remediation team investigated and determined that no data breach had occurred. The system was restored to full functioning, but the business suffered a business interruption.

Total Cost: $183,500 under Computer Attack (for Data Restoration, System Restoration and Loss of Business) + Data Breach Response Expenses (for Legal Review and Forensic IT Review) + Cyber Extortion (for extortion payment/negotiator but ransom not paid)