Westchester®

CYBER CLAIMS SCENARIOS

WHAT WE HAVE PAID LATELY

Westchester's Cyber ERM policy provides industry-leading coverage designed to address evolving regulatory, legal and cybersecurity standards. We understand the risks associated with cyber exposures and use our guiding claims principles to handle claims with integrity, empathy, promptness, expertise and fairness.

Below are some cyber claim scenarios that we have handled and paid recently:

Type of Claim	Details of Claim
Ransomware Attacks	An assisted living facility experienced a "brute force" ransomware attack and had several of its files encrypted. A ransom of approximately $30,000 was initially demanded. After paying a small amount of the ransom demand to obtain a sampling of the decryption tool, the company decided to instead rely on its backups to restore its systems. While no Personally Identifiable Information (PII) was compromised as a result of the attack, several critical systems important to the company became inoperable, including call button systems, security systems and the medicine tracking software. The company incurred losses of more than $250,000 to get the affected systems back on-line as well as an additional $50,000 for the services of a breach coach and forensic vendors.
Ransomware Attacks	A hospital's computer system was the subject of a ransomware attack. While the attacker sought only $500, the cyberattack essentially shut down the medical facility. The hospital incurred significant expenses attempting to restore the data from their computer systems. They could not bill any of the health insurance carriers while the system was affected. Additionally, the imaging capabilities of the hospital were greatly impacted as they could not produce the images from MRIs or CT scans. The malware completely corrupted the hospital's system and they had to resort to paper mode to chart and monitor patients. Lastly, the hospital's payroll system also went down as part of the attack. As a result of the attack, more than $700,000 was paid for forensics, data recovery, business interruption and crisis management costs.

Westchester®
A Chubb Company

Type of Claim	Details of Claim
W2 – Phishing Attack	Insured was the victim of a spoofing attack whereby a bad actor contacted the company's payroll/HR manager impersonating the email address of the company's CEO. Pursuant to the spoofing email, the bad actor requested the company's 2016 W2 forms, which included names, addresses and social security numbers, of the company's current and former employees. Before it was determined that the company was subject to a spoofing attack, the W2 forms were transmitted to the bad actor. Approximately 4,000 current and former employees of the company were affected. Thereafter, a former employee of the Insured, whose personal information was compromised in the breach, filed a class action lawsuit against the Insured alleging that the Insured negligently failed to protect its current and former employees' personal information. As a result of this attack, $70,000 was spent for legal fees, notification and call center services, and credit monitoring. Defense Costs will be covered under the terms of the Policy as well.
Business Interruption Claim	Insured was the victim of a denial of service attack from an unknown source. The attack caused a 22-hour outage to the company's website and a continued degradation of service for an additional 4 days. The incident resulted in the company's inability to sell subscriptions to customers through its website. This event resulted in $750,000 in business interruption losses and an additional $40,000 was spent on forensic accounting services.

CONTACT US

For more information, please contact your local agent or visit www.westchester.com/us/cyber.

Westchester®
A Chubb Company