BRIEF CASE
SPECIAL EDITION

Cyber Security Awareness Month

Cyber Claim Scenarios in Healthcare

The healthcare sector continues to be an increasingly attractive target for cyber criminals. From ransomware attacks that paralyze office operations to data breaches exposing sensitive patient information, the consequences of cyber threats in healthcare can be devastating. The following claim scenarios were supplied by our partner, Tokio Marine HCC - Cyber & Professional Lines Group, as they work with a wide variety of healthcare clients to provide cyber security solutions. These scenarios show the operational and financial impacts of a cyber attack.

Claim Scenario 1: Ransomware Event

The Attack

A healthcare provider with five locations experienced a ransomware attack that encrypted critical systems and disrupted operations across the organization. The attack exploited the widely publicized Log4j vulnerability in VMware Horizon, allowing the threat actor to move laterally across the network and deploy ransomware. As a result, virtual desktops became inoperable, and access to imaging, medical records, and patient scheduling was lost. The insured was unable to access its backups, which had also been compromised.

The Response

Cyber liability insurance coverage was triggered. Breach counsel and forensic investigators were engaged immediately. The original ransom demand of $2 million was negotiated down, and a decryption key was obtained to restore access. The insured suffered significant downtime and had to cancel hundreds of patient appointments.

The Cost

The total costs incurred exceeded $850,000.

OUM CHIROPRACTIC MALPRACTICE INSURANCE

800.423.1504
oumchiropractor.com

Claim Scenario 2: Cyber Extortion Threat

The Attack
A healthcare practice experienced a ransomware attack that impacted three servers and approximately 50 workstations, encrypting systems, and halting operations. The threat actor demanded a $100,000 ransom and claimed to have exfiltrated approximately 80GB of data. The attacker had exploited an open Remote Desktop Protocol (RDP) connection and maintained system access for several days, during which data access and potential exfiltration were observed.

The Response
The incident was reported under the practice's cyber liability insurance policy. Forensics and breach counsel were retained to assess the scope of impact. A ransom payment was negotiated down to $45,000, and the insured was ultimately able to recover operations. The incident caused business interruption and required extensive restoration efforts.

The Cost
Incurred costs totaled just under $250,000.

Claim Scenario 3: Phishing Fraud

The Attack
A healthcare practice discovered that it had been fraudulently induced to issue multiple payments totaling over $1.5 million to a threat actor impersonating several of the practice's legitimate vendors. The fraud was carried out through a targeted phishing scheme that exploited several internal accounts. The attacker successfully inserted themselves into email threads, redirecting outgoing vendor payments to fraudulent accounts.

The Response
Although some funds were recovered through the insured's banking institution, approximately $581,000 remained unrecovered. The insured submitted a claim under its cyber liability insurance. Incident response included forensic analysis of the compromised email accounts and legal support to assess notification obligations, ultimately confirming that no protected data was accessed.

The Cost
Total costs incurred, including forensic and legal services, reached $260,500.

Risk Management Strategies

- **Segment and secure backups.** Store backups offline or on separate networks to prevent compromise during an attack.
- **Encrypt sensitive data.** Ensure data is encrypted to reduce exposure in case of exfiltration.
- **Monitor data access.** Use logging and monitoring tools to detect unauthorized access or data movement.
- **Educate staff on cyber hygiene.** Train employees to recognize phishing attempts and follow secure communication practices.
- **Plan for operational downtime.** Have contingency plans for patient care and scheduling during system outages.

As a healthcare provider, it is critical to make sure you are protected. That's why OUM insureds receive our CyberAssurance endorsement coverage at an annual aggregate limit of $50,000 at no additional cost, per individual.* However, as these cyber claim scenarios show, this isn't always enough to protect your practice from the incurred costs as a result of a cyber attack. If you want to increase your coverage, OUM policyholders are eligible for enhanced cyber coverage at a reduced cost through ProAssurance Agency!

**Coverage is subject to the terms and conditions of the applicable endorsement, including to the annual aggregate limit for any Insured Organization. Policies issued in the states of KS and NY do not include CyberAssurance coverage.*

Disclaimer: The scenarios used are examples of the types of claims and associated costs commonly seen and do not represent a comprehensive explanation of any one particular claim. While the subject coverage is designed to address certain risks and associated costs, coverage may not be available in all circumstances. Each reported claim will be evaluated on a case-by-case basis. The actual policy or endorsement language should be referenced to determine coverage applicability and availability. The information contained in this document does not constitute legal advice, it is for general informational purposes only and is prepared from a risk management perspective to aid in reducing professional liability exposure. You are encouraged to consult with your personal attorney for legal advice, as specific legal requirements may vary from state to state.