HEALTHCARE INDUSTRY INSIGHTS

Cyber Threats Unveiled:

Safeguarding Healthcare Against Ransomware and Cybercrime

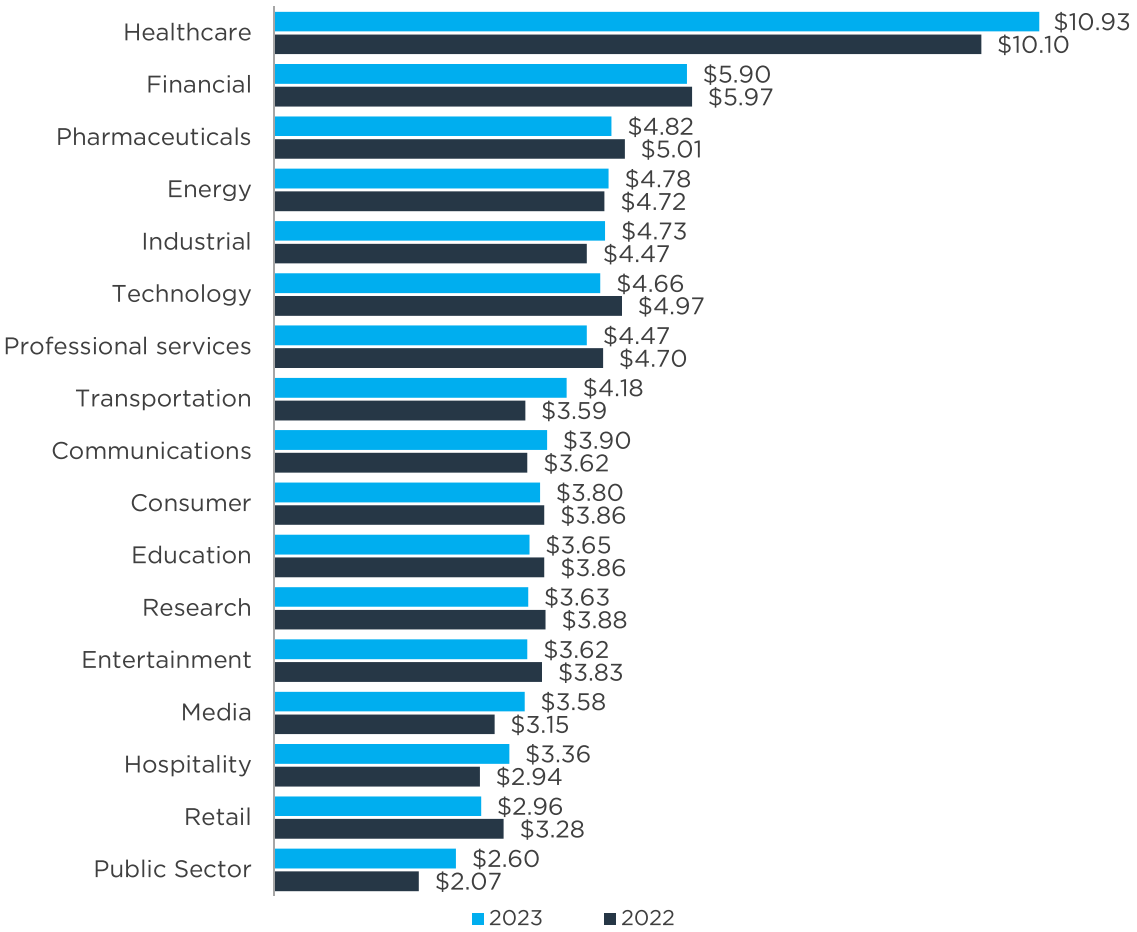
The healthcare industry has become a prime target for cybercrime due to the vast amounts of sensitive data it manages. And cybercriminals have become more sophisticated, making it urgent for providers to obtain comprehensive cyber insurance. Learn about the evolving landscape of cyber threats in healthcare, the types of cybercrime, insurance coverages available, and best practices for safeguarding against these threats.

Healthcare organizations possess a treasure trove of data, including personal identification information (PII) and protected health information (PHI), making them attractive targets. The transition to electronic health records (EHR) and the rise of telehealth have simply increased opportunities for cyberattacks.

According to the Department of Health and Human Services (HHS) Office for Civil Rights (OCR), cyberattacks on healthcare organizations in 2023 set two new records: the most reported data breaches and the most breached records in a single year. The OCR received 725 data breach reports and more than 133 million records were exposed or disclosed.[1]

In fact, healthcare breaches are more costly than in any other industry: The average cost of a healthcare data breach in 2023 was $10.9 million, higher than any other industry and over double the average of all industries ($4.5 million).[2]

Cost of a data breach by Industry



Source: IBM Security: Cost of Data Breach Report 2023

1 HIPAA Journal, "Healthcare Data Breach Statistics," July 18, 2024.
2 IBM Security: "Cost of Data Breach Report 2023," accessed July 25, 2024.

Understanding Cybercrime

To mitigate cybercrime risk, healthcare organizations must ensure they have appropriate insurance coverage. However, prior to deciding what protection you require, it's important to understand the distinct types of cybercrime. The most common include the following:

- **Funds transfer fraud**, which occurs when a cybercriminal directs a financial institution to transfer funds without the victim's knowledge;
- **Social engineering**, when an individual is tricked into transferring funds to an unintended party; and
- **Invoice manipulation**, which stems from a breach, typically through a Business Email Compromise, and results in the alteration of invoices to redirect payments to an unauthorized party. This type of fraud can go unnoticed for extended periods, with criminals remaining in the system for an average of over 200 days.

Evolving Cyber Policies

Cyber insurance policies have evolved significantly, especially with the inclusion of invoice manipulation. Available types of cyber coverages include:

- **Funds transfer fraud and social engineering coverage:** These coverages can be included in a comprehensive cyber policy package and can also be included in commercial crime policies but are sub-limited.
- **Invoice manipulation:** Because it's usually not included in standard cyber policies, coverage for invoice manipulation often requires an additional endorsement, and is typically part of a cyber policy, not a crime policy. It's crucial to request this invoice manipulation cover specifically to ensure comprehensive protection.
- **Utility fraud:** This coverage protects against the unauthorized use of the network for activities like crypto jacking.
- **Ransomware and extortion:** These cover scenarios in which bad actors hold systems hostage or threaten to expose data.

Determining Appropriate Coverage Levels

To assess the necessary level of coverage, healthcare organizations must evaluate individual exposures rather than rely on peer benchmarking alone. Cyber policies typically cover amounts ranging from $250,000 to $500,000 on an aggregate basis for cybercrime. But given the potential financial impact of breaches, it's advisable to have higher coverage limits. Factors to consider include:

- The number of records your organization retains.
- Your organization's record-retention policies.
- The potential financial losses the healthcare institution could face from a breach — including legal, forensic, data breach notification, credit monitoring and public relations costs.

5 Best Practices for Cyber Risk Mitigation and Securing the Best Coverage

1. **Cyber policy provisions and requirements**: It's essential for healthcare organizations to understand the specific provisions and requirements of any cyber policy. For example, many policies include a call back provision that requires verification of transactions for coverage eligibility. Organizations must review and (if necessary) amend these provisions to ensure they have the right coverage or understand the requirements to trigger this cover.

2. **The role of OFAC in cybercrime coverage**: The Office of Foreign Assets Control (OFAC) protects the United States against payments to sanctioned cybercriminals. If an entity on the OFAC list holds data for ransom, insurance cannot and will not cover it.

3. **Regulatory considerations**: Healthcare organizations must comply with various regulations, including HIPAA, FERPA and state-specific requirements. This is especially important for organizations operating across state lines, such as telehealth services. A cyber policy can help in reporting under these regulations and help defend any inquiries by the regulators.

4. **Payment card industry data security standard (PCI-DSS)**: Healthcare organizations must also consider their compliance with PCI-DSS. Breaches affecting payment card data can lead to significant fines based on the volume of transactions processed. It's also crucial for healthcare providers to ensure their third-party vendors are in compliance with PCI-DSS.

5. **Kidnap and Ransom (K&R) policies**: Kidnap and ransom policies may offer extortion coverage as well. If your organization holds a K&R policy, it's worthwhile to review any additional coverage availability there.

Preparation is Key

Healthcare organizations must navigate the complex landscape of cyber insurance to adequately protect against cybercrime, and preparation is key.

Assessing specific risks and coverages, complying with regulatory requirements, and implementing robust policies and procedures are critical steps in mitigating threats. As cyber threats evolve, the strategies and protections to safeguard sensitive data and operations must evolve as well.

To obtain the best coverage, organizations must demonstrate to insurers they have robust policies and procedures. Underwriters assess the strength of these protocols when determining coverage terms and limits.

HUB's healthcare and cyber experts have deep industry expertise to provide personalized risk consulting services to healthcare organizations to help obtain optimal policies and coverage amounts. There is no standard cyber insurance policy that can be applied to every business, so having an experienced broker is important to making sure you're adequately covered.

Contact a HUB healthcare insurance specialist to get started.

Strategic support that puts you in control.

When you partner with us, you're at the center of a vast network of experts who will help you reach your goals. With HUB, you have peace of mind that what matters most to you will be protected — through unrelenting advocacy and tailored solutions that put you in control.

For more information on how to manage your insurance costs and reduce your risk, contact a HUB healthcare insurance specialist.

HUB healthcare insurance

Ready for tomorrow.

Risk & Insurance | Employee Benefits | Retirement & Private Wealth

HUB