VERITAS

Optimize Your Cyber Insurance Strategy

Improve Your Healthcare Organization's Security Posture and Reduce Cyber Insurance Premiums

Ransomware Risk & Rising Costs

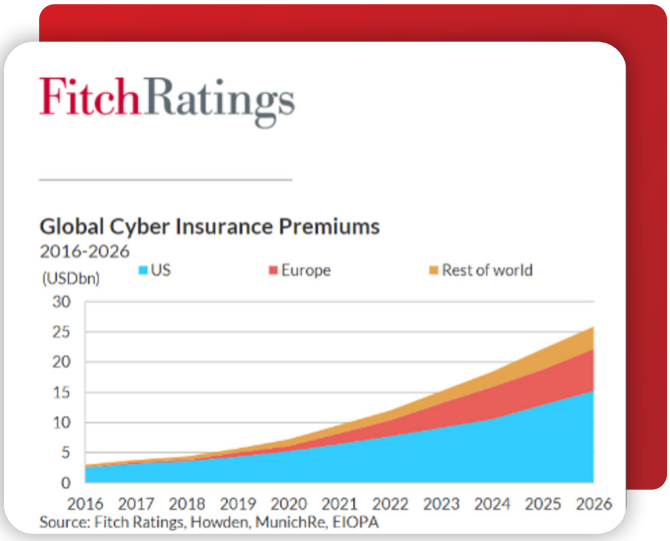
$265B

The cost of ransomware attacks over the next 10 years[1].

As cyber threats increase, the business of cybersecurity has expanded. Every organization is a target. Deloitte predicts over the next 10 years the cost of ransomware will be more than $265B[1]. The healthcare industry has an even bigger target on its back with a 45% uptick in attacks since November 2020, 18 million patient records affected in 2020 (at a cost of $21 billion), and $50 million in revenue lost in a single hospital attack in 2021. It has reached such proportions that in 2021, the Biden administration acknowledged ransomware as a shared global threat for the government and private sector by issuing Executive Order 14028, to "improve the Nation's Cybersecurity." No entity is immune. This escalation in risk has made ransomware a new frontier for insurers, creating a $7.6B cyber insurance industry, which is expected to grow to $36.8B in 2028[2]. Now more than ever, managing risk and the costs associated with it have become an even bigger consideration for healthcare industry leaders.

Reality Check

In Verizon's 2022 Data Breach Investigations Report, ransomware incidents increased nearly 13 percent between 2021 and 2022[3] – that's even bigger than the past five years combined. And even more alarming, the report showed ransomware was present in almost 70 percent of malware breaches in 2021. IDC's 2021 Ransomware Study concluded 37 percent of global organizations experienced an attack[4]. The risks are high. And while cyber liability insurance helps reduce the financial risk, coverage prices continue to skyrocket.



A recent Global Cyber Insurance Market Update by FitchRatings illustrates the staggering increase in cyber insurance premiums year-over year.[5]

Due to the increase in frequency of cyberattacks and the rising cost of ransomware demands, many insurance underwriters left the industry, leaving approximately 20 cyber insurers owning 65-80 percent of the market. To better mitigate their own risk, insurance providers have imposed stricter requirements and stipulations that ultimately push organizations to be better and more resilient. And for the healthcare industry, the stakes and requirements are already high. Today, it is not unusual for organizations like yours to pay four to eight times more for the same amount of coverage— or be denied coverage—if these new requirements are not met. But there is an opportunity for organizations to meet the requirements, reduce risk, and reduce premiums.

Mitigating Risk

With the increasing value of personally identifiable information (PII) and protected health information (PHI) in today's digital infrastructure, it is incumbent upon every organization to find ways to reduce their exposure in the event of a successful cyber attack. Healthcare entities are increasing their focus on managing patient data because of the increase in cyber attacks, exponential data growth, rising expectations, and preparing for unexpected events. Taking such steps also helps organizations qualify for cyber insurance and more reasonable premiums.

1 in 3

Healthcare organizations reported being hitby ransomware in 2020[3].

These actions don't require large budgets or hiring more staff, but they do require a better understanding of how ransomware attacks occur and the best implementation policies that can drastically reduce the ability for cybercriminals to access valuable data. After a data breach occurs, most organizations test and restore their systems. But it may not be enough. However, tearing down and rebuilding a working data system isn't always practical, as it's expensive, time consuming and potentially risky.

But assessing data systems for gaps and vulnerabilities is a strategic way to evaluate system security and future cyber readiness.

Healthcare organizations don't have to tear down to rebuild because there are key tools at their disposal that can go a long way in mitigating their risk. Veritas supports healthcare organizations and policy holders by strengthening their resiliency posture, helping them align to insurance policy guidelines and thereby reducing claim payouts and high premiums.

MAINTAIN CONTROL | *ELIMINATE UNCERTAINTY* | *REDUCE RISK & COMPLEXITY*

Illuminate with Data Visibility

Complete Infrastructure and Data Visibility:
- Edge to Core to Cloud

Across All Major Data Protection Solutions

Adopt Anomalous Activity Detection and Malware Scanning

Near Real-Time AI-Based Anomaly Detection
Automated and On-Demand Malware Scanning
Recovery of Clean Data

Protect All Data from All Sources

Reduce Attack Surface
30+ years Experience with Security Engineered into Products
Gartner Leadership 17 Times

Optimize for Flexible, Rapid, Hybrid Recovery at Scale

Flexible, Hybrid, Rapid Recovery:
- Any Size/Scale Failure
- Anywhere from Anywhere

Recovery from Object Level to Entire Data Center
Recovery Success Rate: 100%

Implement Immutable and Indelible Storage and Air Gap

Immutability Your Way:
- BYO, Appliance, Cloud, and SaaS

Indelibility Using Zero Trust Principles
Built-In Air Gap Solutions
Industry's Only Tamper-Proof Immutability Timer

Orchestrated Rehearsal and Recovery

Non-Disruptive, Cost-Effective Recovery Rehearsals
Tier *"0"* to Tier *"N"* Application Recovery with Varying RPO

How to Get the Most Out of Your Cyber Insurance

Insurance is a necessary expense and part of the cost of doing business. The goal is to keep the expense low while having the best protection should the worst occur. But odds are not in your favor. Cyber insurance companies provide a financial safety net, but it's important to note that insurance policies may not cover the full cost of an attack. Healthcare organizations can't afford to be complacent just because they're insured. The costs can be staggering. For example, if a healthcare entity had a ransomware attack which stole 100,000 patient data records, the healthcare organization could be hit with a class action lawsuit resulting in $2,000 per patient settlement. This would amount to a $200M price tag -- which may not be covered under the policy unless the premiums were extraordinarily high. Attacks are becoming more frequent and costly, but partnering with the right cyber insurer and technology solutions provider to map out a resiliency and business continuity strategy can help make your organization better manage its risk and policy premiums. Here are four key areas to address in your strategy:

Access Management

Attacks can be significantly reduced when a comprehensive access management process is in place that controls and manages who can do what in a system. Insurers seek policyholders that can track and log all actions taken by users with Administrator credentials and editing rights, such as enterprise administrators, service accounts, domain administrators, global administrators, hybrid identity administrators, and privileged role administrators. Since many healthcare organization employees are not all centrally located in a specific building or geo, a sound access management strategy is critical. Additionally, cyber insurers want transparency and authentication measures for third parties or managed service providers (MSPs) accessing the network remotely because it improves security. And all appropriate security measures must be taken to ensure patients that access healthcare sites are who they say they are.

Security

Security is top of mind for everyone and anyone responsible for managing and protecting data. Attacks and accidents can and do happen, which is why cyber insurers require policyholders to take a holistic approach to security. Given that healthcare now creates more data than any other industry, security is a top priority. Endpoint security and protection is one area that insurers focus heavily on when signing up a new policyholder or assessing an insurance claim. Insurers also seek to understand how authentication occurs for employees and vendors, what security tools are used to protect emails and endpoints, and how network security is achieved when applications sit on-prem and in the cloud.

Software and Hardware Management

While not always top-of-mind for organizations, when there isn't a sound software and hardware management process in place, significant risks are present. Healthcare organizations need to be cognizant of what happens with their end-of-life/support hardware and software. Are updates required? Does decommissioning need to occur? Does certain software need to be segregated from the rest of the network?

This is important for end-of-life platforms as well as the servers and workstations running on them. Cyber insurers want to know how often patch management occurs in the environment, which is a best practice that all should follow.

Resiliency

Resiliency can be costly and complicated. Cyber insurers are extremely focused on resiliency as it is the foundation for business continuity, and can serve as a guide to improve an organization's overall data and cloud management strategy. Important questions that healthcare organizations should ask themselves are:

- How often is critical information being backed up?
- Where are the backups stored?
- Is the backed up information quickly accessible?
- What data is being backed up?
- Does the organization have a business continuity plan?
- Does the organization have recovery time objectives (RTO) in place?
- How often does the organization perform disaster recovery drills?
- Is the policy holder/applicant able to test the integrity of backups prior to restoration to be confident that they are free from malware?

Veritas Supports Policy Holders and Cyber Insurers

There should be true collaboration between cyber insurers and policy holders as they rely on each other for success. Cyber insurers are very prescriptive in their guidelines and requirements around security and resiliency. The key to optimizing your healthcare cyber insurance coverage is to demonstrate how your organization is actively engaged in reducing its risk from attacks both on-prem and in the cloud. Reduced risk translates to reduced claims and lower premiums.

Veritas works with cyber insurance companies and is often recommended by them because we surpass their data management and protection requirements by enabling healthcare organizations to demonstrate their end-to-end recoverability and resiliency approach.

For policy holders, our experts work with you prior to and during insurance-led risk assessments to prove your risks are controlled through resiliency and immutable storage capabilities. This proactive approach helps healthcare organizations comply with policy requirements and manage insurance costs.

Cyber insurance is here to stay. Investing in your cyber-resiliency solutions now can save on insurance premiums immediately and greatly reduce the risk of costly data breaches later.

Why Veritas

Veritas is uniquely equipped to help healthcare organizations of all sizes conquer the complexity of managing and protecting their business critical data. Our approach closes the gaps in your ransomware resiliency with a proven strategy aligned to the National Institute of Standards and Technology (NIST) framework. We also help you meet HL7 compliance, HIPAA compliance, PHI laws, meaningful use standards, and more—as well as giving you a head start on meeting any future requirements. Additionally, our integrated product portfolio, unified data management experience, and proven track record of recovering nearly 100 percent of data after cyber-attacks solidifies Veritas as an industry leader—from edge to core to cloud.

Veritas is an industry member of the U.S. Department of Homeland Security (DHS) Cyber Information Sharing and Collaboration Program and actively working with DHS to mitigate global cyber threats. Through this program Veritas supports DHS's focus on enabling actionable, relevant, and timely unclassified information exchange through trusted public-private partnerships across all critical infrastructure (CI) sectors. We are committed to preventing ransomware attacks across our 80,000 customers around the world. To that end, Veritas delivers the most comprehensive technology ecosystem you can find. It's trusted by many of the world's largest companies, including 95 percent of the Fortune 100. The Veritas unified Cloud Data Management Platform lets you take control of all your enterprise data and applications across any cloud, any environment at scale. Our integrated approach to data management and protection is proven to deliver unmatched versatility, performance and cost-savings. Now's the time to discover what we can do for your healthcare organization.

1. Defending against ransomware in an age of emerging technology
2. Fortune Business Insights report, titled, "Cyber Insurance Market, 2021-2028"
3. 2022 Data Breach Investigations Report
4. IDC's 2021 Ransomware Study: Where You Are Matters!
5. Global Cyber Insurance Market Update

About Veritas

Veritas Technologies is a leader in multi-cloud data management. Over 80,000 customers—including 95 percent of the Fortune 100—rely on Veritas to help ensure the protection, recoverability, and compliance of their data. Veritas has a reputation for reliability at scale, which delivers the resilience its customers need against the disruptions threatened by cyberattacks, like ransomware. No other vendor is able to match the ability of Veritas to execute, with support for 800+ data sources, 100+ operating systems, 1,400+ storage targets, and 60+ clouds through a single, unified approach. Powered by Cloud Scale Technology, Veritas is delivering today on its strategy for Autonomous Data Management that reduces operational overhead while delivering greater value. Learn more at veritas.com. Follow us on Twitter at @veritastechllc.

VERITAS

2625 Augustine Drive
Santa Clara, CA 95054
+1 (866) 837 4827
veritas.com

For global contact information visit:
veritas.com/company/contact

V1682 12/22