Confronting the New Economics of Cybersecurity with Risk Automation

With the proliferation of ransomware, healthcare delivery organizations (HDOs) are reckoning with a 'new math' in cybersecurity and its impact on the business of healthcare. Over the last decade, cyber threats have evolved with ever-greater malignancy and now seek to shut down care operations itself. Not surprisingly, regulatory fines and cyber insurance premiums are skyrocketing, while ransomware continues to put patient safety at risk and drain the coffers of even well-managed HDOs.

To confront the new economics of cybersecurity, leading organizations are increasingly automating their cyber risk management to help prevent, mitigate, and recover faster from these potentially catastrophic cyberattacks. Here are five key benefits of cyber risk automation and the associated return on investment (ROI) of each:

Reduce Risks to Patient Safety and Downtime of Care Operations

In many cases, the overall financial impact of a breach can be significantly determined by how fast the organization can respond and recover from the incident. A cyberattack on a hospital costs, on average, $45,000 per hour of downtime from lost business[1], increasing the imperative to quickly understand what happened; where and how it affects your IT environment and patient care; and who, where, and how it affects all third and fourth parties. Without automation and the real-time risk visibility it affords, getting answers to these questions (and resolving all issues) can take days, weeks, even months – costing millions.

What's more, with 40% of breaches caused by third parties[2], the failure of the status quo can be traced back to a lack of comprehensive risk coverage across two vectors:

1. Most often, vendors are only assessed at procurement, not across the entire contract lifecycle.
2. Only perceived "high-risk vendors" are assessed, not all discrete sources of cyber risk across the enterprise.

With third-party risk automation, HDOs can assess all sources of risk across their entire lifecycle, including vendors, products, services, supply chain, IRB/research, medical devices, affiliates & practices, and internally-developed applications. As the scope of risk changes throughout the lifecycle – due to implementation, configuration, integrations, updates, retirement, etc. – automation enables quick and accurate reassessment of changes in risk posture and can automatically generate and track new remediations required.

RETURN ON INVESTMENT:
For a typical 500-bed hospital, faster incident response saves $45,000 per hour, and comprehensive risk coverage can help prevent a third party breach, which costs over $10 million on average[3].

Accelerate Innovation Adoption and Its Benefits

Providing the highest quality of care has always been at the heart of healthcare's mission and innovation is core to this success. From software to services, the average hospital now has over 1,500 vendors[4], with 10-15 connected medical devices per bed[5]. The number of vendors per HDO is expected to grow 30% year-over-year[6], promising continued gains in clinical and business performance. But, despite heroic efforts, CIOs/CISOs have had little success keeping up with the demand for innovation.

Security teams face not just an increasing volume of vendors, but growing complexity in the risk assessment process itself, driven by rapid release schedules, the proliferation of "smart" devices, and ever-increasing calls for interoperability and integration. As a result, risk assessments now take 45-60 days to complete on average. This equates to foregoing $2.0 million per month in return on investment from new innovations, stalling enhancements to care delivery, operating efficiency, and overall organizational performance.

Resource-constrained, leading CIOs/CISOs are automating third-party risk management processes to handle the increasing volume and complexity of vendors. Within a week, these HDOs see assessment completion times cut down to 5-10 days, with enhanced risk visibility, analysis, and accuracy. Upon reassessment, automation can drive down completion time by 90%, to only a few days, and, in many cases, down to just a single click.

RETURN ON INVESTMENT:
Accelerating innovation adoption by more than a month through third-party risk automation enables a typical 500-bed hospital to pull forward $2.0 million in return on investment.

Force-Multiply FTE Productivity and Workforce Engagement

Like a perfect storm, just as demand intensifies to assess more vendors with higher complexity, an acute talent shortage hits hard. The cold conclusion is that healthcare CIOs/CISOs will need to do more with less for the foreseeable future. Already, many leading organizations are turning to cyber risk automation to help alleviate the current imbalance in supply and demand, and are seeing significant benefits:

- Elimination of time-consuming and costly manual tasks throughout the entire third-party risk management process
- Force-multiplication of security team productivity, enabling each employee to assess more vendors in less time with higher accuracy
- Elevation of staff to 'top-of-license', resulting in higher job satisfaction and morale
- Stronger recruiting results by capturing more diverse skill sets and offering a modern work environment compatible with the "new normal", hybrid workforce
- Redeployment of scarce security resources to higher-value work and initiatives

RETURN ON INVESTMENT:
A typical 500-bed hospital sees 300% improvement in productivity through risk automation, equivalent to 2-4 FTEs.

Flatten the Cyber Insurance Cost Curve

With cyber insurance premiums increasing 30-50% every year[7], HDOs are urgently looking for ways to stop the bleed on cost. What's worse, many organizations find out the hard way that they are essentially 'self-insured' in the wake of a catastrophic breach, as the rising cost of lawsuits, lost business, and penalties often far exceed their policy liability limits. To contain cost growth and mitigate the financial fallout of a breach, HDOs must effectively demonstrate and communicate to insurance carriers that they are indeed *less risky*. Doing this requires:

- Aligning with industry standard frameworks such as NIST CSF 1.1 and HICP, and automating all relevant workflows including self-assessment, evidence capture, corrective action plans, and reporting to prove framework coverage levels.
- Minimizing third-party risk through fully-automated risk assessment and reassessment of all vendors & products throughout the entire contract lifecycle, including medical devices, IRB, and supply chain.
- Benchmarking to show how security operations, investments, and NIST CSF coverage compares to peer organizations – demonstrating above-average security performance to insurance carriers across multiple cyber risk categories.

Lack of a robust program that systematically measures and manages cyber risk often leads to above-average premium increases, or even claim denial. With most insurers now asking targeted questions about how your HDO manages third-party and enterprise risk, it is critical to prove to cyber insurers that you are making (and have made) all efforts to maximize the strength and resilience of your security program to lower your overall risk profile. Those that do report below-market rate increases with an effective 20-30% savings versus the market.

RETURN ON INVESTMENT:
For a typical 500-bed hospital with a $1M premium, this translates into $200-300K in annual savings.

Reduce Regulatory Fines and Actions

While the *average* penalty imposed by HHS for HIPAA violations is $1.2 million[8], in recent years, many cases have seen substantially higher sums, usually after a long audit and an agreement to comply with a detailed corrective action plan. With the threat landscape and attack surface growing faster than most HDOs can manage, many CIOs/CISOs have come to believe that it's a matter of "if, not when" for their organization.

In January 2021, public law 116-321 was passed where HHS must take "recognized security practices" such as NIST Cybersecurity Framework (NIST CSF) and Health Industry Cybersecurity Practices (HICP) into account when assessing HIPAA violations by business associates and covered entities. While not safe harbor, if organizations can demonstrate coverage for at least 12 months, HHS can:

A. Mitigate fines

B. Result in early, favorable termination of an audit

C. Mitigate settlement remedies

Cyber risk automation enables HDOs to create a centralized, longitudinal risk record to demonstrate their adoption of NIST CSF and/or HICP and prove 12 months of use to HHS, if (or when) needed.

RETURN ON INVESTMENT:
For a typical 500-bed hospital, demonstrating coverage of "recognized security practices" such as NIST CSF and HICP in the event of a breach may result in reduced fines and penalties from HHS, which currently average $1.2 million per HIPAA violation.

Final Thoughts

With ransomware now representing an existential threat to healthcare, the imperative to bring order to chaos through automation across cyber risk management has never been greater. AHA Cybersecurity Preferred Solution Providers such as Censinet provide a fully-automated third party and enterprise risk management solution to help prevent, mitigate, and respond faster to today's cyber threats.

If you would like to learn more, contact us at info@censinet.com or visit https://www.censinet.com

SOURCE:

1. **Perspectives in Healthcare Security**, Ipsos, Sept 2021
2. **U.S. Department of Health and Human Services**, Office for Civil Rights, Breach Portal available at https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
3. **Cost of a Data Breach Report 2022**, IBM, July 2022
4. The Impact of Ransomware on Healthcare During COVID-19 and Beyond, Ponemon Institute, September 2021
5. **Fierce Healthcare**, "82% of healthcare organizations have experienced an IoT-focused cyberattack", Heather Landi, Aug 29, 2019
6. The Impact of Ransomware on Healthcare During COVID-19 and Beyond, Ponemon Institute, September 2021
7. **Cyber Insurance: Action Needed to Assess Potential Federal Response to Catastrophic Attacks**, United States Government Accountability Office, June 2022
8. **U.S. Department of Health and Human Services**, Office for Civil Rights

Censinet is an American Hospital Association Preferred Cybersecurity Service Provider for Cyber Firm Risk Management and Information Governance and Cyber Risk Assessment, Privacy and HIPAA Compliance.