Making the Case for Risk Transformation in Healthcare

Healthcare IT, security and risk leaders must embrace five key business case elements to secure the funding needed to transform their cybersecurity programs

Given rapid changes in digital health and growing threats to patient care, risk programs are in need of an overhault to keep pace with the threat landscape and the ever-increasing volume and technical diversity of third-party vendors. Transforming cyber risk management to meet these challenges will require significant resources and investment across the next decade.

As IT, security, and risk leaders, we often struggle with developing a compelling business case for risk management transformation to secure this critical funding. While traditional metrics remain important – ROI, cost, and efficiency – leading organizations are thinking in broader terms when making the case for transformation: *How does cybersecurity impact the overall business and patient safety?*

Making the Case for Transformation

Securing the resources and investment for risk transformation requires a business case that links back to the business of care. Here are five strategic objectives to consider when developing a compelling business case for risk management transformation in healthcare:

1. Connect Your Risk Program Vision with the Business

All too often, security and risk leaders communicate using technical language that non-technical leaders don't intuitively understand. Business leaders are more likely to support a vision when the components and objectives are understandable to them and relevant to the organization's long-term strategy and mission.

For example, risk program leaders can demonstrate how additional resources and investment will create (a) a lasting reduction in the disruption to care operations, (b) meaningful improvement in quality and safety metrics, and, (c) faster, more accurate due-diligence of risk for M&A activity and affiliations.

2. Drive Cross-Functional Coordination and Consolidation

Most healthcare organizations manage a dozen or more risk functions. Each of these functions creates siloed resources, independent processes, and additional tool costs. As part of your transformation, strengthen cross-functional governance using an enterprise risk steering committee to ensure decisions aren't made in a vacuum. Executives, legal, finance, clinical, supply chain, information technology, GRC, information security, and business continuity should all be represented in the decision-making process.

Look for opportunities to consolidate risk management tools and fully automate third party risk assessments, supply chain, risk reporting, remediation tracking, and incident response. Demonstrate how automation enables the organization to spend time on higher-value activities in a more secure way such as faster supply chain throughput, accelerated innovation adoption, and higher-quality research/IRB. Simply put, if you're still using spreadsheets to manage risk twelve months from now, odds are your predecessor won't be in month thirteen.

3. Focus on Resilience and Business Continuity

If we've learned anything over the last few years, it's that healthcare is woefully under-resourced to handle "black swan" events such as catastrophic ransomware attacks. We must do a better job of developing a prioritized roadmap that clearly identifies all threats to business continuity and hold ourselves accountable to remediating any and all security gaps that could be exploited to shut down operations.

By linking targeted remediations to business, technology, and environmental drivers, we can demonstrate better organizational preparedness and resilience. An agile RiskOps program supports business outcomes rather than solely protecting the data infrastructure. It enables security and risk teams to conduct regular vulnerability assessments of the enterprise as a whole, and take action before events occur.

4. Incorporate Recognized Industry Best Practices

In Jan. 2021, the Health Information Technology for Economic and Clinical Health Act (HITECH) was amended to require the Secretary of Health and Human Services (HHS) to consider "recognized security practices" of covered entities and business associates when making certain determinations. While not "safe harbor", if your organization can prove 12 months of adherence to these recognized security practices, such as NIST Cybersecurity Framework (NIST CSF) and/or HHS 405(d) Health Industry Cybersecurity Practices (HICP), HHS must consider this when making determinations. This, in turn, can mitigate fines for violations; result in an early, favorable termination of an audit; or mitigate conditions in resolution agreements.

5. Adopt a "Stronger Together" Strategy

In the last few years, we've seen ransomware increasingly shut down care operations and extort millions from healthcare organizations. These attacks are well-coordinated, so why aren't we? It's no surprise that in a recent poll, the majority of CIOs and CISOs selected "Leveraging a Network of Providers to Remediate Risk" as the approach most likely to have the greatest impact on cybersecurity across the healthcare industry.

When transforming your risk program, incorporate active collaboration strategies with peers to effectively counter these well-orchestrated attacks. A 'Stronger Together' mentality leverages peer remediations, best practices, and shared intelligence to counter threats to patient care, data and operations. How can we work together as providers, payers, and vendors to share information and actions that collectively creates a more secure and productive healthcare ecosystem for all?

Conclusion

Following these five principles can facilitate your risk transformation journey and serve as a guide to continuous improvement in risk program outcomes to protect patient safety and business operations. By aligning risk program needs with the needs of the business, you can gain Board and executive-level support for the long-run.

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

KLAS RESEARCH CENSINET MEASURED Cybersecurity Transparent

American Hospital Association™ Preferred Cybersecurity Service

CHIME

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.