From Server Room to Operating Room: Today's Cyber Risk is Enterprise Risk

More than ever, healthcare providers rely on software technology, connected devices and a third-party ecosystem of vendors and suppliers to deliver high-quality care to patients. However, patient safety and care operations are under an ever-increasing risk of cybersecurity attacks and incidents. No longer is the threat just about the loss of protected health information (PHI); Cyber attacks such as ransomware directly threaten patient safety.

Healthcare leaders and boards must manage cybersecurity as an enterprise risk in order to safeguard their mission of safe patient care. Properly managing cyber risk within the enterprise requires an integrated, proactive strategy. Managing and communicating cybersecurity risk as enterprise risk is a complex undertaking. Today, every aspect of a healthcare organization's enterprise operates within a technology context. Healthcare delivery organizations (HDO) leaders must consider the digital dependencies across clinical and business processes.

Here's a 5-step strategic blueprint for creating a unified front against cybersecurity risks across the healthcare enterprise:

STEP ONE: Govern cybersecurity as enterprise risk

A culture of cybersecurity must start at the top. Unfortunately, senior executives and board directors are not cybersecurity experts, and many security leaders do not articulate cybersecurity risk in a way that aligns with an organization's enterprise risk management approach. Framing cybersecurity risks in a "language" that healthcare leaders can understand is important for meaningful risk decisions.

The first step is to elevate cybersecurity risk in the broader context of its overall mission and business objectives, and not just as a technical issue. This establishes a baseline for overall governance with alignment of business objectives against cybersecurity risks to patient safety, care delivery, business operations, data, and reputation. Business Impact Analysis (BIA) can be used to quantify the impact on the business while qualifying the criticality of the process or asset using a defined tiering approach. Regulatory requirements are reviewed and mapped to appropriate business goals and objectives.

STEP TWO: Identify all business processes and supporting assets across the enterprise

Once governance processes and procedures are established, make a list of all business processes and associated digital and physical assets needed in support of those processes. Take note of any legacy processes that may be managed independently or winding down during the transition to a replacement process. Below are a few example business processes:

- Innovation
- Digital health for consumers
- Telehealth
- Research/Institutional Review Board (IRB)
- Operational - Business
- HR, employee time & payroll
- Financials, revenue & reimbursement
- Physical plant and related services
- Operational - Clinical
- EMR, labs, and radiology
- Inpatient and Outpatient (Ambulatory Care)
- Patient & Clinical Support Services

Once business processes and assets are identified, organizational roles and responsibilities may need to be realigned. Leadership teams and stakeholders must clearly define roles and map responsibilities, including documenting the names of responsible personnel, across all clinical and business functions, risks, audit, security, and technology.

STEP THREE: Inventory all third-party suppliers, vendors, and products

Effectively balancing the risks and benefits of technology with enterprise goals and objectives requires a dynamic, prioritized digital inventory of assets, risks, and risk dispositions (e.g. accept, transfer, avoid) aggregated and reported at the enterprise level. A centrally managed digital inventory enables the stakeholders to easily record, aggregate, normalize, prioritize, and communicate cybersecurity risks and decisions in the context of enterprise risk.

An effective way to digitally inventory and manage all third-party vendors, suppliers and products is through an automated risk management platform. These tools enable you to centrally capture, manage, and maintain information about the asset (e.g. vendor information, product name, contract information, cost, business impact, tier criticality, business associate status, regulatory obligations, data security agreements, etc.) in a single place. These tools help ensure clear and consistent communication among other groups and functions that support risk management, such as human resources, legal, auditing, and compliance.

STEP FOUR: Assess cybersecurity risk across the enterprise

All connected "things" are subject to cybersecurity attacks, whether it's an infusion pump, radiology system, or mobile-based scheduling application. Non-technical suppliers such as a hospital's laundry service are equally susceptible to an attack which can cripple its ability to operate. Additionally, cyber risks may exist outside traditional IT processes such as institutional review boards (IRB), affiliated practices, and joint ventures/M&A —any business process that relies on digital data must be assessed for cyber risk.

Cyber risk must be assessed across the enterprise to include third-party vendors, non-technical suppliers, partnering covered entities, medical non-technical suppliers, and internal policies, procedures, and controls. Leveraging standard frameworks and practices such as the NIST Cybersecurity Framework and Health Industry Cybersecurity Practices (HICP) can help drive completeness, efficacy, and assessment benchmarking across industry peers.

A "set it and forget it" approach to assessing cyber risk is no longer sufficient. Internal procedures, third-party cloud applications and connected medical devices are updated more frequently today than ever before. Cyber risks must be continuously and dynamically assessed, across the lifecycle of the contract, vendor relationship, and product scope—from cradle to grave and all points in between.

For example, risk at the point of purchase will most likely be different from risk associated with implementation and technical configurations. Changes to usage can also introduce new risks if, for example, the initial scope of a cloud-based application did not include regulated data but six months later users were found adding PHI records. Monitoring for real-time updates to data and access scope, and conducting annual reassessments will drive the needed insight to stay on top of risks that may develop throughout the business process or vendor relationship.

STEP FIVE: Implement practices and controls to protect, respond to, and recover from cyber threats

Once cyber risks are identified and analyzed, the final step is risk disposition. Tools can be used to automatically generate recommended mitigations and remediations for risk reduction. These "corrective actions" guide the effective implementation of technical, physical, and administrative controls.

For example, privacy and security controls such as encryption and multi-factor authentication can protect regulated data and critical systems to support confidentiality, integrity and availability. Effective disaster recovery and business continuity policies and procedures ensure that operations recover with little to no downtime in the event of a ransomware attack.

Summary

Effective management of cybersecurity risk is a shared enterprise responsibility and must involve the people, processes, and technologies that protect the mission and goals of the enterprise. By managing cybersecurity as enterprise risk, the healthcare organization establishes a common framework, language, and reporting methodology among operational and leadership teams. Additionally, cybersecurity and enterprise risk practitioners can drive meaningful discussions on gaps, requirements, and priorities that establishes cybersecurity risk as an important element of effective enterprise risk management.

It takes courage to move an organization forward. The inertia surrounding change makes it easier to argue the "why not" versus the "why" when discussing cybersecurity. Consequently, continuing to manage cybersecurity as technical, and not enterprise risk ends up being the biggest risk of all.

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

KLAS RESEARCH CENSINET MEASURED Cybersecurity Transparent

CHIME

American Hospital Association™ Preferred Cybersecurity Service

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.