TEVORA™ | White Paper

Refining Third-Party Risk Management in Healthcare Organizations: Addressing the Epidemic

July 2023

Introduction

Healthcare organizations across the globe have been embracing purpose-built technology to deliver high-quality care to patients, whether virtually, in person, or through at-home services. Patients have been digitized effectively through the vast array of new devices, applications, and monitoring technologies that give physicians an unprecedented view of each patient's health; however, this does come at a cost – both literally and figuratively.

Current State of Healthcare's TPRM Landscape

In 2022, the healthcare sector suffered nearly double the number of third-party breaches in 2021 and accounted for almost 35% of all incidents noted in the year[1]. Patient data shared amongst vendors, an increasingly interconnected network of Internet of Things (IoT) devices, and an abundance of outdated software have created numerous third-party vulnerabilities for threat actors to exploit and the consequences are only becoming more devastating:

Healthcare vendors have the highest disclosure time period:

169 days on average[1]

Noncompliant with HIPAA and HITRUST

Average cost of a data breach within healthcare:

$10.1 M[2]

Highest of all industries for the 12th year in a row

For midsize hospitals, a cyberattack costs about

$45,700 per hour[3]

Supply chain vulnerabilities were responsible for

62% of all system intrusion incidents in 2022[4]

Compliance Challenges

Being considered critical infrastructure by the U.S. government makes the healthcare sector one of the most heavily regulated industries in terms of security and privacy requirements. Although enacted to drive security initiatives towards better-protecting healthcare systems, with most organizations already heavily constrained, keeping up with these constantly evolving frameworks becomes challenging.

For example, the U.S. Department of Health and Human Services (HHS) issued a new bulletin on December 1, 2022, clarifying the applicability of HIPAA's Rules to include tracking technology vendors. This bulletin comes out following the growing number of litigations where tracking technology vendors were found to be collecting patient health information from both websites and mobile applications in violation of HIPAA's Rules. This example is one of the many instances where healthcare organizations and providers find themselves in a reactive position, attempting to reevaluate currently active contracts and technologies to remediate potential noncompliance. Extrapolate this issue among all applicable regulations (e.g., GDPR, PCI DSS, ISO 27001), and it is not difficult to see why healthcare organizations are struggling to stay ahead.

Insurance Premiums

In addition to litigations following data breaches and fines imposed per compromised record, healthcare organizations also pay some of the highest cybersecurity insurance premiums. With a significantly higher number of breaches than any other sector and no signs of slowing down, insurance underwriters are accounting for this increased risk by charging exorbitant premiums. According to the 2022 National Association of Insurance Commissioners *Report on the Cyber Insurance Market,* "underwriters are more cautious in examining an insured's risk presented by the third parties" as the significant increase in supply chain attacks has proven "companies are not effectively managing third-party risk."[5] This further constrains the security budgets available to healthcare organizations, reducing the ability to invest in vital technologies and resources. If this trend continues, healthcare organizations will continue to be the favored targets of financially motivated threat actors due to the weaker defenses and higher probability of paying ransoms-which either further increase insurance premiums or result in bankrupted hospitals requiring federal intervention.

Transition from Triaging to Preventative Care

The third-party ecosystem in healthcare needs improvement, but how exactly is that achieved? It is essentialto recognize that change cannot occur overnight. Third-party risk management is an ongoing lifecycle and will not be implemented in the same way amongst

different organizations. Each step should lead toward increased maturity that aligns with the organization's long-term business strategy; however, there are initial steps that organizations should take to create a solid foundation.

Perform Diagnosis

The first step an organization must take towards evolving its third-party risk management program is to establish an accurate inventory of all third parties - treatment cannot be rendered until the full scope of the problem is understood. These relationships should be classified as this will help establish prioritization and the type of risks relevant to that relationship. Criteria to consider may include:

System Access: Does the third party have access to critical systems, networks, or infrastructure? Are services that may impact patient care, medical devices, or other operational services provided?

Data Sensitivity: Does the technology or services provided involve access or transmission of sensitive data, such as PII, PHI, or IIHI?

Regulatory Compliance: What regulations apply to this third party? Are they currently meeting compliance requirements?

E.g., is a Business Associate Agreement (BAA) in place if PHI is disclosed to the third party?

With an inventory established and critical criteria for each engagement mapped, the healthcare organization can begin efficiently prioritizing and targeting similar third-party groupings for remediation. Depending on available resources, this can take various forms ranging from only engaging those that constitute immediate regulatory or security risks to formally assessing all third-party relationships with more scrutiny. As reassessing existing vendors is often more challenging since there is already an established contract, it is more effective to wait until contract expiry to perform a thorough risk assessment and incorporate new requirements.

Developing Long-Term Resiliency

As initial actions should be underway to improve an organization's third-party ecosystem, it is essential to maintain a long-term strategy to avoid falling back into a reactive posture. This means adopting a synergistic framework to match business goals with third-party risk management improvements. Again, this may vary between organizations. However, a universal goal within the healthcare industry is to align with HITRUST – one of the most rigorous cybersecurity frameworks that incorporate many other relevant regulations and

frameworks. Using HITRUST as the target for eventual certification provides measurable parameters to evaluate the TPRM program against. This assists in demonstrating maturity progress to internal stakeholders while assuring external entities, such as cybersecurity insurance providers or partners.

Among the 19 domains stipulated by the HITRUST Common Security Framework (CSF), domain 14 outlines the controls specific to Third Party Assurance. Depending on where the organization's maturity and long-term goals lie, the TPRM program goals can adjust to match the roadmap toward compliance:

For i1 certification, the number of controls required is fixed and does not vary per organization, as implementation status is only to be considered.

For r2 certification, the number of controls is specific to your organization, and the assessment looks at the policy (15%), procedure (20%), implemented (40%), measured (10%), and managed (15%) aspects of each control.

Periodic Program Maturity Assessments or HITRUST Gap Assessments can then be performed to evaluate progress toward HITRUST certification, and any deficiencies documented with Corrective Action Plans. By following this iterative process towards compliance, healthcare organizations benefit by efficiently planning maturity improvements, recognizing measurable success with metrics, and reducing friction within the business when implementing TPRM processes.

Prescribing the Right TPRM Solution

As progress is made toward long-term TPRM maturity, healthcare organizations will inevitably run into manual processes and bottlenecks that hinder the overall program. In the same way, manually reviewing all logs generated within an organization cannot be a viable long-term solution, so is manually managing all third-party relationships.

TPRM solutions should be evaluated and considered when developing maturity roadmaps to determine the optimal time for investments. A common misstep many organizations may make is to invest in a solution before a formal TPRM program has been developed.

Not all TPRM solutions are built to solve the same problems. Examples of the various types of solutions available include:

Questionnaire Automation: Tools designed to speed up the questionnaire process by incorporating conditional logic, weighted risk flagging, email notifications, and other features to streamline the assessment process.

Security Rating Services: Ongoing external scanning tools that ingest both proprietary data and other external threat intelligence sources to provide a high-level assessment of the third party's security posture.

Workflow Management: Tool for operationalizing logical tasks, organizing to create a streamlined process, and delegating ownership to the correct individuals to ensure all stakeholders stay informed.

TPRM Platform: General platform for identifying, managing, and treating known risks within an organization with reporting capabilities tracking risk management activities.

Supply Chain Management: Tools to identify and manage risks with subcontractors or software providers existing within the organization's broader supply chain.

Some tools may possess a combination of capabilities (e.g., Security Rating Service with Questionnaire Automation components), and some may have niche functionality not listed above that could be relevant to achieving your organization's maturity objectives. Due to this fractured environment of third-party solutions, it is critical to build your TPRM program tailored to your organization and then consider how the available options may best integrate with the maturity roadmap and existing technological investments.

Conclusion

As healthcare organizations continue to provide the highest quality care with the latest technological innovations, any associated risks should be evaluated and treated. Allowing an interconnected healthcare landscape to proliferate third-party vulnerabilities is a gamble that healthcare organizations and their patients can no longer afford to take. By investing in a robust TPRM program as part of a holistic security initiative, healthcare organizations can safeguard highly sensitive information they are entrusted with, protect the lives that rely on high operational uptime, and fortify their attack surface from costly data breaches, regulatory fines, and cybersecurity insurance premiums.

How Tevora Can Help

If your healthcare organization needs assistance or support with designing, building, implementing, assessing, or operating a tailor-made TPRM program, our team of security experts is ready to help. Throughout this article, we emphasize the importance of creating a program specific to your organization's needs, we extend this notion to our services as well. We will connect you with healthcare specialists knowledgeable of common regulatory pitfalls faced in the industry to ensure your TPRM program is effective and successful.

If you have questions or would like to connect our team of security professionals, please just give us a call at (833) 292-1609 or send us an email at sales@tevora.com. We look forward to partnering and supporting your cybersecurity efforts.

References

1. Third-Party Breach Report by Black Kite: https://blackkite.com/whitepaper/2023-third-party-breach-report/
2. IBM Cost of Data Breach Report https://www.ibm.com/downloads/cas/3R8N1DZJ
3. Adams, K. Healthcare data breaches by the numbers: 9 stats. Becker's Health IT. March 23, 2022. Healthcare data breaches by the numbers: 9 stats (beckershospitalreview.com)
4. 2022 Data Breach Investigations Report. Verizon. 2023 Data Breach Investigations Report | Verizon
5. National Association of Insurance Commissioners Report on the Cyber Insurance Market https://content.naic.org/sites/default/files/cmte-c-cyber-supplement-report-2022-for-data-year-2021.pdf

Our team is ready to discuss your specific challenges and identify the best solutions.

Give us a call at (833) 292-1609 or email us at sales@tevora.com.

TEVORA™

Go forward. **We've got your back.**