Deloitte.

Revitalizing health care with a dose of resilience

Why a modern approach to TPRM is critical to your company's health

Introduction

In today's rapidly evolving macro environment, the health care sector faces unprecedented challenges. The industry relies heavily on an intricate ecosystem of suppliers, vendors, and third parties to provide essential care to patients. Consequently, disruptions in this ecosystem may have severe repercussions. It's time to move beyond traditional compliance-focused methods and modernize third-party risk management (TPRM) to incorporate resilience and continuity of care.

Why resilience is being prescribed

Does my TPRM framework include resilience considerations? That's a question you should be asking if you aren't already. Resilience is more than just a buzzword; it is a strategic imperative. Resilience is about knowing what is essential and having confidence that you may continue to provide core services during a disruption. It's about more than just having dual systems; it's also planning so that those systems are not co-located to avoid simultaneous failures. Think of it as stationing the right people with the right mindset to navigate disruptions and recover quickly. While you cannot predict all scenarios, preparing for the most realistic events contributes to a resilient organization.

The criticality of resilience in TPRM

The health care sector is especially vulnerable to disruptions due to its reliance on third parties. Organizations in these sectors depend on an ecosystem of suppliers, vendors, and other third parties to run their businesses and deliver care to patients, making them particularly susceptible to disruptions.

In the health care industry, "a matter of life and death" is not an idiom; it's a reality, as even minor disruptions can affect continuity of care, significantly having an impact on patient well-being. The critical nature of care delivery makes TPRM more crucial in this industry than in others. Resilience adds an extra layer of protection on to the TPRM strategy. It is essential to ensure that organizations are prepared for disruptions and can quickly recover. Organizations should evaluate current TPRM frameworks for resilience integration, remediate gaps, and develop scenarios to validate third-party resilience.

The uphill task of strengthening resiliency

Organizations can face several common challenges in their journey to strengthen resiliency. Addressing these challenges requires a strategic approach that formalizes processes, establishes tracking systems, and integrates third-party life cycle (TPLC) processes. Common challenges include siloed approaches, limited documentation, and manual updates. Improvement opportunities include formalizing processes, establishing tracking systems, and integrating TPLC processes.

High-profile third-party cyber incidents have demonstrated vulnerabilities within the supply chain. Imagine what can happen to surgical devices and surgical procedures that rely on a complex network of vendors that may inadvertently bring along cybersecurity risks. These disruptive events highlight the need for response strategies. Therefore, organizations should consider applying resiliency leading practices and broad response strategies to address supply chain vulnerabilities and commit to continuous monitoring and assessment of third-party cyber risks to maintain resilience.

What a modern approach to TPRM looks like

The traditional approach to TPRM has predominantly been compliance focused. However, in the health care industry, it is imperative to modernize TPRM strategies to prioritize resiliency and continuity of care. This modernization is crucial to mitigate disruptions caused by the macro environment and third-party failures, with the intent of helping organizations to maintain their operations and patient care effectively. A robust TPRM program should not only meet compliance requirements but also provide operational resilience during disruptions. Some characteristics that define an effective and modern TPRM program include:

1. **Tier-based approach:** A tier-based approach involves categorizing third parties into different tiers based on the level of risk they pose and the impact of their services on the organization. High-risk vendors, such as those with access to sensitive data or supporting critical operations, are placed in higher tiers and receive more rigorous oversight and management. This prioritization helps ensure that the most critical vendors are closely monitored and managed, while lower-risk vendors receive proportionate attention.

2. **Resilience-focused contracts:** Contracts with vendors should include specific clauses that address resiliency and business continuity. These clauses might require vendors to have disaster recovery plans, conduct regular testing of these plans, and ensure that they can quickly resume services after a disruption. By embedding these requirements into contracts, organizations can hold vendors accountable for their preparedness and ensure that they are capable of supporting the organization during adverse events.

3. **Alignment with recovery time objectives (RTOs):** RTOs are the maximum acceptable lengths of time that critical business services can be down after a disruption. Leading TPRM programs determine whether vendors' recovery capabilities are aligned with these RTOs. This means that vendors need to be able to restore their services within the time frames required by the organization to maintain continuity of critical operations. This alignment is crucial for reducing downtime and ensuring that essential services remain available.

4. **Continuous risk monitoring:** Continuous risk monitoring involves the ongoing assessment of vendor risk profiles using various data sources and advanced technologies like generative artificial intelligence. This process includes tracking key risk indicators (KRIs) that signal potential issues, such as financial instability, cybersecurity threats, or compliance breaches. By continuously monitoring these indicators, organizations can detect emerging risks earlier and take proactive measures to mitigate them before they escalate into significant problems.

5. **Fourth-party consideration:** Fourth-party risk management extends the scope of TPRM to include the vendors' subcontractors or partners (fourth parties). This involves assessing the risks associated with these fourth parties and understanding how they might affect the primary vendor's ability to deliver services. By considering fourth-party risks, organizations can gain a more detailed view of their supply chain and address potential vulnerabilities that could affect their operations.

6. **Risk assessment and scenario planning:** Risk assessment, clinical and operational continuity scenario planning: Regular risk assessments involve systematically evaluating the potential risks posed by vendors and identifying areas of vulnerability. Clinical and operational continuity scenario planning complements this by developing and testing hypothetical scenarios to understand how the organization and its vendors would respond to various disruptions. This practice helps organizations prepare for different types of incidents, such as natural disasters, cyberattacks, or supply chain disruptions, test and enhance their existing clinical and operational-focused continuity plans, and support their efforts to have effective response capabilities in place.

To support this modern approach, health care organizations should leverage advanced tools and capabilities to gain broad risk insights across various domains, including cybersecurity; regulatory compliance; financial health; and environmental, social, and governance risks. They should collaborate with internal and external stakeholders to analyze critical business services, document gaps in current resilience capabilities, create a remediation roadmap, and analyze risks to prioritize actions based on potential impact and likelihood.

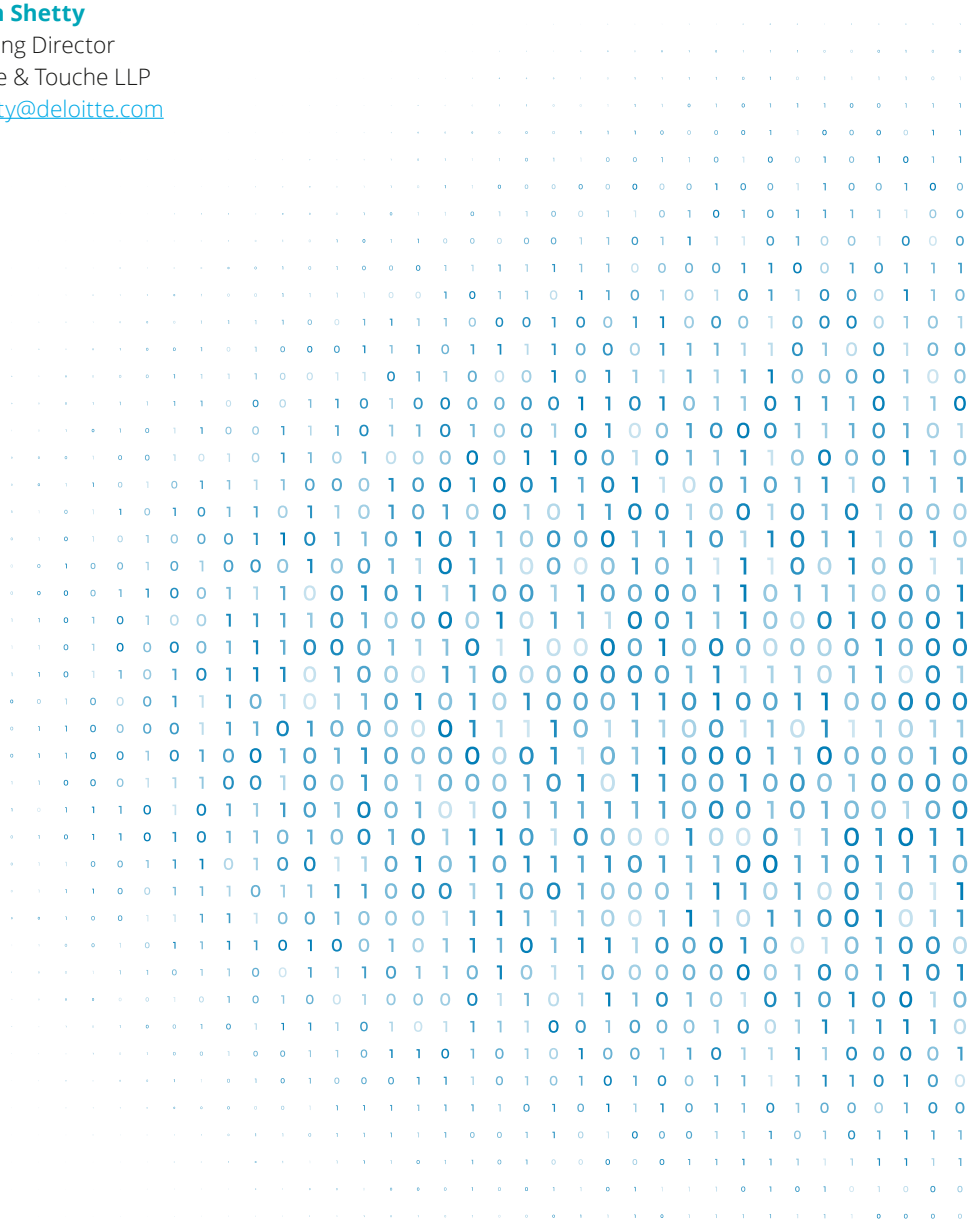
Building trust and having confidence in capability

Building and managing resilience is critical in an ever-changing landscape. Health care organizations should look to enhance their TPRM programs to comply with regulations, build trust, and maintain recovery confidence. This proactive approach can enable health care providers to provide uninterrupted care, even in the face of disruptions. By adopting these strategies, health care organizations can significantly improve their TPRM while providing resilient and continuous care delivery. Ultimately, the focus should be on building capabilities rather than merely conducting paper-based exercises. This capability-driven approach ensures that organizations are not just compliant but genuinely resilient, ready to respond to and recover from various scenarios effectively.

Authors

Steph Meehan
Partner
Deloitte & Touche LLP
stmeehan@deloitte.com

Mitesh Shetty
Managing Director
Deloitte & Touche LLP
mishetty@deloitte.com



Deloitte.