Measurability: Cybersecurity Ratings for Third-Party Risk Management in the U.S. Healthcare Sector

William Yurcik[†‡]
Centers for Medicare & Medicaid Services (CMS)
Baltimore, MD USA
[0009-0004-8453-3898]

Stephen North
Infovisible
Oldwick, NJ USA
[0000-0002-1087-1577]

O. Sami Saydjari
Dartmouth College
Hanover, NH USA
[0009-0001-3241-887X]

Gregory Pluta
University of Illinois
Urbana-Champaign, IL USA
[0009-0004-4760-1441]

***Abstract*—We share experience implementing cybersecurity metric-based algorithmic ratings to proactively manage the third-party cybersecurity risk within a large critical national infrastructure – the U.S. healthcare sector. The U.S. healthcare sector is currently estimated to be about 17.6% of the U.S. economy as measured in GDP, and is the U.S. top employer accounting for about one in three new U.S. jobs and 13% of total U.S. employment [1,2].**

In February 2024, a cybersecurity attack on the Change Healthcare pharmacy clearinghouse became a seminal third-party risk event when a single outage had an outsized impact felt nationwide for a significant period of time. We describe what happened, why the impact was outsized, what were the responses, and lessons learned.

After the Change Healthcare event, cybersecurity ratings are playing a larger role leading to the proactive identification of vulnerabilities in third-party service providers, the continuous monitoring of third parties for changes in security posture, and the use of cybersecurity ratings to track third-party remediation efforts. Lastly, we share examples of how cybersecurity ratings can be used to provide enhanced protection for critical third-party infrastructure and how cybersecurity ratings can be used to calculate return-on-investment (ROI).

Keywords— healthcare third-party risk, healthcare supply chains, supply chain security, cybersecurity rating

I. INTRODUCTION

An organization's security posture is only as strong as its weakest link. External partners, vendors, suppliers, and contractors - who often have access to sensitive data and systems - can become that weak link. Third-party risk management (TPRM) is important because it protects an organization from the wide range of risks introduced by outsourced organizational functions to external partners, vendors, suppliers, manufacturers, and contractors.

TPRM is a subset of the broader category of supply chain risk management (SCRM) [3]. Third-party risk focuses on managing direct relationships with any external entity that an organization relies on, while supply chain risk is concerned with all the issues pertaining to the entire end-to-end network of suppliers, manufacturers, distributors, and the flow of goods and services contributing toward the end product or service produced by the first-party organization. Table 1 is a comparison of TPRM versus SCRM highlighting that TPRM is focused on issues under direct control of an organization while SCRM includes broader supply chain issues such as severe weather events, geopolitical issues, macroeconomic issues, and terrorism.

TABLE I. TPRM VERSUS SCRM

Feature	*TPRM*	*SCRM*
Scope of Focus	Direct relationships with external organizations, such as vendors, contractors, and service providers. This includes IT and cloud service providers, payment processors, and other business partners.	The entire ecosystem of suppliers and processes required to deliver a product or service, including all upstream and downstream partners. SCRM considers risks throughout the whole value chain, not just direct suppliers.
Visibility	Risks associated with the directly contracted third parties. Third-party actions or security posture directly affect the first-party.	Seeks to understand risks that can originate anywhere in the extended network, including vendors' vendors (known as fourth-parties).
Primary Risk Types	Emphasizes cybersecurity and compliance risks because third-parties may have access within the first-party enterprise security boundary depending up integration. Other risks include operational, legal, financial, and reputational/brand.	Covers a broader range of risks, including geopolitical events, natural disasters, financial instability, operational issues, raw material shortages, and labor concerns across the entire supply network.
Risk Ownership	First-party is directly responsible for managing all the risks introduced by third parties.	First-party is responsible for ensuring the entire supply chain remains resilient, even though individual risks may arise from vendors outside of direct relationships.
Key Concern	The security posture, compliance, and overall reliability of all external third parties with established direct contractual relationships.	Continuity and resilience of the entire flow of goods and services supply chain, and how a disruption anywhere in the chain will impact first-party end product/services.

Before proceeding further, we define terminology to be used throughout the rest of the paper. We use a hospital as the organization in context:

- **First-Party:** a hospital
- **Second-Party:** a hospital patient
- **Third-Party:** A vendor to a hospital with a direct contractual relationship to provide a product or service
- **Fourth-Party (or Nth-Party):** A vendor or subcontractor that a 3rd-party vendor uses, but with whom the hospital has no direct relationship

[†] Corresponding Author <william.yurcik@cms.hhs.gov>; [‡] Organizational Disclaimer: "The views presented herein do not represent the views of the Federal Government."

Figure 1. First, Third, and Fourth/Nth Parties

For purposes of this paper, we will be using explanatory instances, both actual and hypothetical, from the healthcare sector. Healthcare providers depend heavily on global supply chains for medical devices, essential pharmaceuticals, and digital health tools enabling supply chains to provide timely treatments and efficient operations. However, supply chains containing external partners, vendors, suppliers, manufacturers, and contractors also introduce significant risks.

The remainder of this paper is organized as follows: Section II presents different third-party risk frameworks that may be used as a basis for a TPRM program. Section III provides a brief overview of a general TPRM program. Sections IV introduces examples of actual real-world disasters caused by an Nth-party showing that TPRM is not an academic exercise. Section V introduces quantitative cybersecurity ratings as an automated way to scale TPRM continuous monitoring for real world situations. Section VI applies TPRM to the U.S. healthcare sector to share an example case study of scalable TPRM continuous monitoring. We end with a summary in Section VII.

II. THIRD-PARTY RISK FRAMEWORKS

A TPRM framework establishes guidelines for identifying, assessing, managing, and mitigating risks from external vendors. It ensures third parties meet security and compliance standards, protecting organizations from data breaches, operational failures, regulatory violations, and reputational damage. A range of TPRM frameworks/standards exist, each with a different purpose, scope, and target audience, including but not limited to the following:

- "Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations" U.S.-focused (NIST SP 800-161 rev1) for overall supply chain security [4,5]
- "ISO/IEC Information for Supplier Relationships" international standard in 4 parts: ISO 27036:1/2/3/4 [6,7,8,9]
- "FDIC/FRB/OCC Interagency Guidance on Third-Party Relationships" - risk management designed specifically for the banking industry across the entire life cycle of their relationships with third-parties, from planning and due diligence to monitoring and termination [10]
- "Third Party Risk Association (TPRA) GuideBook" [11]

The most suitable framework for an organization depends on its specific industry, operational maturity, and strategic goals. With the wide range of TPRM frameworks, organizations can adapt standards to fit their specific industry sector and risk profile.

III. TPRM PROGRAMS

To ensure third parties operate securely and effectively by managing outsourced data and processes, organizations need a robust TPRM program. Stakeholders, including customers, board members, and regulators, expect mature TPRM programs to be in place.

Figure 2. Common Components of a TPRM Program [12,13]

Figure 2 provides an overview of TPRM program components. Planning and oversight provide an organization with the foundation to build upon and properly support their overall program [12]. Precontract and due diligence ensures the organization performs due diligence commensurate with the level of inherent risk, to determine if the organization should proceed with a specific third-party relationship and prior to signing a contract to ensure business needs will be met [12]. Contract review ensures the organization documents relationship expectations in an agreement that can be upheld in a court of law [12]. It also ensures risks noted within the due diligence process can be addressed within contractual clauses [12]. Continuous monitoring requires the organization to assess third-party risk on a continual basis to ensure contract terms, business obligations, legal and regulatory requirements, and performance expectations are met [12]. Disengagement ensures the organization is able to transition away from a third-party with minimal impact should the relationship end due to contract expiration or when adverse/unplanned conditions are met [12]. Continuous improvement is an ongoing activity which seeks to enhance the organization's TPRM program as third-party risk management guidance, trends, and techniques are realized [12].

TABLE II. THIRD-PARTY RISK TYPES [12,13]

Reputational	Operational	Trans-actional	Compliance	Cyber	Financial	Strategic
Negative public view related to dissatisfied customers, interactions not consistent with institutional policies, inappropriate recommendations, security breaches resulting in disclosure of customer information, and/or violations of law and regulations.	Caused by inadequate or failed processes, people, or systems.	Service/ product delivery issues or third-party performance failures may occur due to inadequate capacity, technology failure, human error, or fraud.	Outcomes resulting from breaches of laws, rules, regulations, or non-compliance with internal policies.	Results from the exposure or loss of data due to technical a failure, human error, or malicious attack.	Results from a Third-Party's failure to meet or align with organizational monetary requirements and expectations.	Results from failing to align strategic goals to business objectives and/or an activity that jeopardizes strategic objectives.

Table II describes the different types of TPRM risks that arise from external relationships, encompassing categories such as Reputational (brand damage), Operational (service disruptions), Transactional (breach of contract), Compliance (regulatory violations), Cybersecurity (privacy breaches and IT system disruptions), Financial (vendor instability), and Strategic (misaligned goals). Another key risk is Concentration (over-reliance on a single vendor). Managing these risks requires a comprehensive TPRM program with ongoing due diligence and continuous monitoring.

In the next section we show that TPRM programs are needed in order to protect organizations from disaster events caused by Nth-parties because ***an organization is ultimately responsible for the actions or inactions of all its third-parties/Nth-parties.***

IV. Real-world Third-party Incidents

Real world third-party risk events have demonstrated that relying on external partners, vendors, suppliers, manufacturers, and contractors can create significant vulnerabilities the have resulted in significant operational disruptions and financial losses. Threat actors increasingly target third parties to exploit weaker security defenses and gain indirect access to more secure organizational enterprise networks.

As third-party risk events have become more frequent and sophisticated, they are evolving from isolated privacy data breaches to systemic supply chain attacks that can cripple economic sectors. Major incidents have demonstrated how a single third-party, or Nth-party can endanger a critical national infrastructure.

A. Disaster Events

TABLE III. NOTABLE THIRD-PARTY INCIDENTS

EVENT	*TYPE*	*DESCRIPTION*
Target (2013)	Cyberattack, Reputational	Hackers gained entry to the Target enterprise network by compromising the credentials of a third-party vendor, Fazio Mechanical Services, and used that access to steal the payment and personal data of over 100 million customers.
Solar Winds (2020)	Cyberattack	SolarWinds (a provider of network/system monitoring software) confirmed that it had been penetrated by a threat actor who inserted malware into software updates of its Orion platform; 18,000 customers installed this compromised update containing malware which was then used to exfiltrate data and covertly spy.
Colonial Pipeline (2021)	Cyberattack, Operational	A threat actor compromised a Colonial Pipeline VPN account access and then encrypted data, demanding a ransom. In response, gas pipelines operations were shut down for several days to prevent ransomware from causing further damage. The shutdown led to localized fuel shortages, panic buying, and significant disruptions across the eastern U.S.
Suez Canal Blockage (2021)	Operational	Massive container ship ran aground wedged diagonally across a single-lane section of the Suez Canal blocking all ship traffic, demonstrating how a single event by one third-party could trigger significant cascading failures across global supply chains.
Toyota Plant Shutdowns (2023)	Operational	System malfunction of database server used to process parts orders shut down 14 assembly plants in Japan. The root cause resulted from insufficient allocated disk space after routine maintenance, not a cyberattack.
CrowdStrike (2024)	Operational	Faulty software update caused a massive global IT outage, leading to a "Blue Screen of Death" (BSOD) on Windows operating systems worldwide, crippling essential services in airlines, healthcare, and finance for days, not a cyberattack.
Change Healthcare (2024)	Cyberattack, Operational, Strategic, Financial	Ransomware attack on a single pharmaceutical clearinghouse triggered a massive third-party risk event, demonstrating how a single cyberattack on a critical vendor could disrupt the entire U.S. healthcare pharmaceutical system.

Table III describes the most significant third-party incidents that have occurred in the past dozen years, there are too many others to provide a comprehensive list.

B. Change Healthcare (2024)

To illustrate an important point, we would like to further explore the most impactful third-party incident to date, the Change Healthcare event of February 2024 (the last incident listed in Table III). A cybersecurity ransomware attack on Change Healthcare, the nation's largest pharmacy claims clearinghouse, triggered a nationwide outage that disrupted prescription drug processing, delayed treatments, and created severe cash flow crises across hospitals, pharmacies, and suppliers [14].

As one of only two major pharmacy switches in the U.S., Change Healthcare represented **a single-point-of-failure** for the entire U.S. healthcare system. The breach—enabled by stolen employee credentials, the absence of multi-factor authentication, and outdated backup systems—crippled prescription distributions for weeks [14]. UnitedHealth, Change Healthcare's parent company, was forced to provide $8.5 billion in emergency loans, while CMS accelerated Medicare and Medicaid payments to prevent insolvencies [14]. Despite these interventions, hospitals reported revenue declines of up to 17% in early 2024, and the attack ultimately exposed the protected health information of 190 million Americans, the largest nationwide documented breach to date [14].

This event underscores the need for greater resilience in healthcare supply chains. Stakeholders must prioritize system segmentation, modernized backup capabilities, and tested business continuity plans to mitigate disruption. **Just as the Federal Reserve provides liquidity support in financial crises, healthcare organizations require contingency mechanisms to preserve operations during cyberattacks.** The Change Healthcare incident serves as a warning that concentrated performance chokepoints and single-points-of-failure in infrastructure can amplify cyber risk into systemic disruptions with broad societal and economic consequences [15].

V. TPRM Measurability through Cybersecurity Ratings

A. What is a Cybersecurity Rating?

The late healthcare cybersecurity pioneer Ross Anderson emphasized in 2006, "Risks cannot be managed better until they can be measured better"[16]. Nineteen years later, cybersecurity metrics have matured, allowing enterprises to use these measurements, although imperfect, to make informed decisions through algorithmic cybersecurity ratings, enhancing operations and investments.

NIST defines a metric as a measurement tool that supports human decision-making to enhance cybersecurity performance [17]. Cybersecurity metrics lack a standard best practice, as they are shaped by individual enterprise environments and the staff responsible for implementing cybersecurity operations. Figure 3 shows possible cybersecurity metrics, some of which are in common use.

In everyday life, assessment rating systems (or indexes) based on underlying metrics are in ubiquitous use to assess complex systems such as human physical health, national economies, and financial instruments.

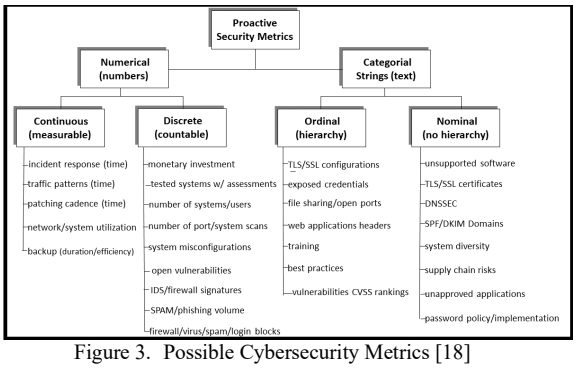

Figure 3. Possible Cybersecurity Metrics [18]

Cybersecurity ratings aim to summarize an organization's overall security posture using measurable metrics. Ideally, this would result in a single, intuitive number representing the enterprise's cybersecurity status at any given time. Presented with the rating for an organization, an analyst can decide whether to further investigate the underlying metrics for that organization or move on to evaluate other organizations.

A Cybersecurity Rating is a data-driven dynamic measurement of an organization's cybersecurity performance used to manage enterprise and third-party cyber risk.

While a cybersecurity rating represents a snapshot at a specific point in time, the trend in the rating over an extended period is of greater significance. Is the rating relatively stable? going up? going down? is there a gradual or drastic rating movement over time? Professionals in the securities, credit, and insurance sectors place a high priority on these trends to effectively evaluate risk. Consequently, we employ longitudinal "sparklines" to display the variation in cybersecurity ratings over a one-year timeframe. Figure 4 illustrates a sparkline depicting the fluctuations in a cybersecurity rating throughout the year, with a shaded rectangle indicating the expected "technology industry range" where similar organizations should ideally maintain their rating.

Figure 4. Cybersecurity Rating Sparkline Over a One Year Time Period [19]

Cybersecurity ratings have been validated against actual attacks. One study found that lower ratings correlated with a higher probability of successful cybersecurity attacks [20].

B. *Toward Continuous Monitoring of Third-Party Risks*

Perhaps the most challenging TPRM problem is that the number of third-party participants is typically large and grows exponentially at each level of separation from the first-party. All it takes is for one third-party among the exponential number to be compromised for the first-party enterprise to be at risk.

Figure 5. Fourth-Party Exponential Growth

While organizations rely on a complex ecosystem of third and fourth parties, perfect monitoring of all Nth-parties is impossible with limited resources. Prioritization of parties into multiple tiers with different levels of monitoring makes it possible to match an organizational risk profile.

Figure 6 contrasts a linear TPRM process with a non-linear TPRM process incorporating feedback based on continuous monitoring results such that vulnerability findings and new threats can be addressed with remediation.

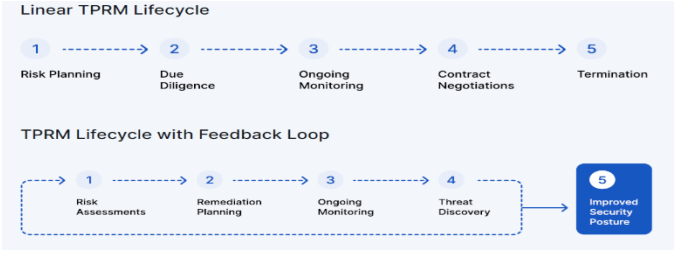

Figure 6. Linear TPRM versus TPRM with a Feedback Loop [21]

Continuous monitoring can play a transformative role in helping an organization understand its unique third-party risks. Instead of reacting to incident disruptions, continuous monitoring can help first parties anticipate and prepare for potential issues.

C. *Different TPRM Dashboard Approaches*

At present circa 2025, there are four major dashboard approaches to communicate TPRM information to human analysts.

Figure 7 shows a first approach which is a scrollable row list of N-Party (redacted) entities, each with assigned cybersecurity rating and a longitudinal sparkline showing rating trends over the last year.

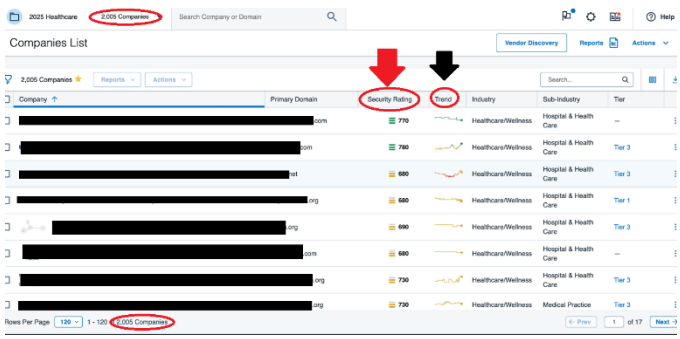

Figure 7. Cybersecurity Rating System Dashboard [19]

Figure 8 shows a hierarchical block dashboard approach. The assessment for each Nth-Party evaluates different categories in order to provide an overall color-coded and letter-graded risk score based on identified vulnerabilities.

Figure 8. Hierarchical Scorecard with Color Codes & Letter Grades [22]

Figure 9 shows a dashboard for a financial quantification approach which attempts to quantify financial risk. Each Nth-Party represents the estimated known loss event frequencies and corresponding loss event financial magnitude such that a quantified financial risk value can be assigned to each Nth-Party. The financial value assigned to each Nth-Party may help decide Nth-Party monitoring prioritization strategies.

Figure 9. Financial Quantification Dashboard [22]

Figure 10 shows a dashboard for a concentric ring hybrid approach combining Nth-Party scoring and financial risk assignment. The outer ring indicates wide scoring ranges, and inner histograms indicate financial risk values. This approach is most valuable in being able to present larger volume Nth-Party information in one dashboard view (without scrolling). However, as the number of Nth-Party entities scale, information on each specific Nth-Party is more difficult to discern.

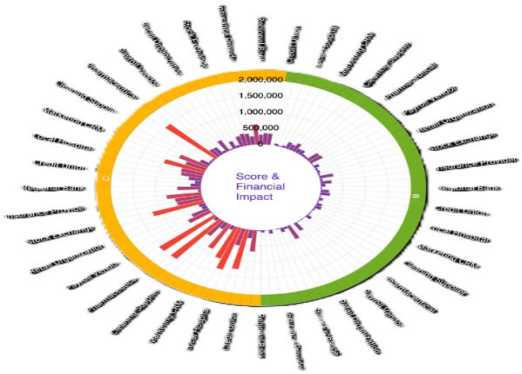

Figure 10. Concentric Ring TPRM Dashboard: Scoring & Financial Loss [23]

VI. AN EXPLANATORY CASE STUDY: THIRD-PARTY RISK MANAGEMENT FOR U.S. HEALTHCARE

We will now present a TPRM case study to share practical implementation details for a real-world scenario – the U.S. Healthcare system. Threat actors are increasingly targeting healthcare vendors and third-party suppliers as entry points into larger healthcare networks [24]. Healthcare, which relies heavily on outside providers for billing, telehealth platforms, and critical software, is particularly at risk.

Figure 11. Fourth-Party Exponential Explosion [25]

A. Understanding Your Supply Chain

Healthcare supply chains are typically large and diverse, creating many potential entry points. A compromise in even a small third-party supplier can lead to extensive system outages and data breaches of personally-identifiable information (PII) and protected health information (PHI), both of which are protected by Federal HIPAA[1] laws.

The healthcare supply chain is one of the two major expenses in healthcare (the other being labor) and it typically operates unnoticed - until there is a disruption. Cyberattacks on a healthcare supply chain pose significant risks. A shortage of essential medical supplies can delay or disrupt patient care. On a wider scale, healthcare supply chain disruptions cause shortages of essential drugs, personal protective equipment, and surgical instruments. Hospitals often pay premium prices for alternative suppliers, straining budgets and procurement teams. These disruptions add financial and reputational risks and weaken trust in vendor relationships [26].

The healthcare sector is unique because of the span of services provided, number of stakeholders involved, and its complexity requiring specialized equipment and supplies. Thus, a well-managed supply chain is critical to the health care sector. Figure 12 is a simplistic view of the U.S. healthcare supply chain. There are many different parts of the healthcare system and each part is heterogenous requiring different input supplies.

The healthcare supply chain is evolving from a cost-focused model to more resilient, patient-centric system powered by advanced technology. The COVID-19 pandemic highlighted weaknesses like "just-in-time" inventory and centralized manufacturing, prompting new strategies for stability.

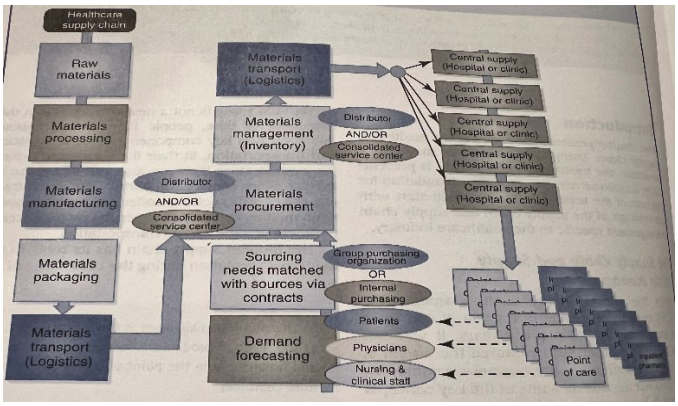

Figure 12. A General Depiction of the Healthcare Supply Chain [26]

Supply chains for different industry sectors have their own special characteristics and this is certainly true with the healthcare supply chain. The healthcare supply chain is different from other industry sector supply chains in six distinct ways: [26]

1) The consequences of supply chain failure may lead to loss of life. The consequence of this difference is that providers pay the additional cost to hold "safety stock" inventory, contract premium levels of transportation, and contract premium service level agreements.
2) Healthcare is highly regulated at both the state and federal levels. Staff must have state-certified qualifications. Facilities must be both state-certified and pass national Joint Commission inspections. Equipment and medical devices must be certified by the Federal U.S. Food and Drug Administration (FDA).
3) Healthcare supply chains have an extremely wide range of variations. For example, some commodity supplies (e.g., laundry, food) are basic to manage while other specialized healthcare inputs (human organs to be transplanted) require the most detailed, specialized management.
4) Many of the assets utilized in the delivery of a service by a hospital are not directly controlled by the hospital itself. The best example is that hospitals provide privileges to surgeons to operate in their operating room spaces and surgeons independently schedule use of the hospital operating room spaces. While hospitals would like to optimize operating room space utilization with scheduling, they do not control surgeon scheduling of operations. There is a fragile détente between hospitals and surgeons since surgeons do provide large revenue streams back to the hospital.
5) Healthcare purchasing is typically dependent on Group-Purchasing Organizations (GPOs). In other industries group purchasing is not commonly used, in other industries it is more common for partnerships to form between suppliers and industrial entities.
6) In measuring supply chain performance, healthcare providers are typically benchmarked against their peers. In other sectors performance benchmarks are generally used across industries. For instance, hospital customer service is measured against customer service at peer hospitals while banking customer service is measured against customer service across all industries.

Figure 13 presents an overview of the healthcare value chain, which encompasses activities that create and deliver healthcare services and products to patients [27]. Unlike a simple supply chain, the value chain focuses on processes that add value and improve patient outcomes, such as research, clinical care, and financial management. Key stakeholders include patients, providers, manufacturers, and payers.

[1] HIPAA = Health Insurance Portability and Accountability Act of 1996 is the federal law that sets national standards to protect the privacy and security of PII and PHI.

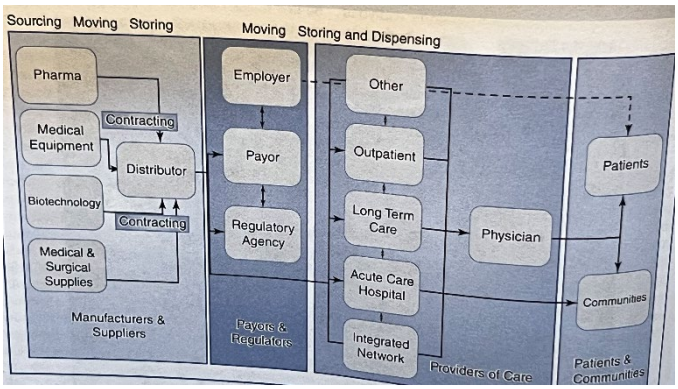

Figure 13. General Depiction of the Healthcare Value Chain [27]

B. Practical Tips to Get Started With Your Supply Chain

To start managing third-party risk you must identify the first-party entity and third-party entities.

The first-party is a perspective of relationships. Any organization can be a first-party and thus all other parties will be viewed in context to their relationship to the identified first-party.

Given the many aspects of U.S. healthcare, we considered analysis options and decided upon hospitals as the best first-party to study in more depth since it is a central convergence point. Hospitals touch every part of the industry including patient healthcare management, most providers have hospital privileges, and hospitals are typically the parent organization of subsidiary activity such as ancillary out-patient services/facilities.

After the first-party is identified, partner organizations within the first-party security boundary must be identified. These may be contractor companies and contract employees who work within the first-party security boundary. For all intents and purposes these partner organizations need to be treated as first-party entities to be assessed with the first-party.

Next, entities must be identified who have contractual relationships with the first-party and are outside of the first-party security boundary. These third-party entities will be entered into the TPRM process including initial assessment and continuous monitoring. It may not be possible to originally assess and continuously monitor all third-party entities depending on the number of third-parties and the resources invested in TPRM.

There are two techniques to identify third-party entities.

One technique to identify a third-party is to reactively wait over time for new organizational contracts to be signed between the first-party and vendors, suppliers, manufacturers, and contractors. At contract signing, there is an opportunity to on-board the third-party signatory into the organizational TPRM process. If you have a large supply chain and do not know where to start this is a good option. Eventually over time, contracts with all third-parties will need to be re-signed and complete third-party TPRM coverage will have happened.

A second technique is to attempt to proactively identify third-parties that may confer the most risk to the first-party and then on-board these third-parties into the TPRM process in priority order by risk level. This second technique is a strategic approach that with accurate third-party selection may provide the most risk reduction in the quickest time. However, identifying the risk levels of different third-parties is difficult given incomplete information before they are analyzed as part of the TPRM process.

Third-party entities must be interrogated to determine the scale of 4th-party entities. Just like third-party entities, it may not be possible to originally assess and continuously monitor all fourth-party entities depending on the number of fourth-parties and the resources invested in TPRM.

The common troubleshooting technique of unplugging a cable to see who is disconnected is referred to as the "*cable swap test"* or *"testing with a known-good cable test"*. This cable swap test is useful for identifying Nth-parties who otherwise may be unidentified/unknown. If it can be done in a controlled setting without impacting production services, different possible Nth-parties can be disconnected (blocked) in order to see if the party in question does in fact has an Nth-party relationship to the first-party, and if it does then what, if any, effect this Nth-party disconnection has on first-party operations.

Nth-party identification is important for the reason we previously highlighted in the 2024 Change Healthcare incident. Healthcare providers, in general, did not know that Change Healthcare existed until the incident occurred, and more importantly did not realize that Change Healthcare represented a single-point-of-failure to their pharmacy operations. The lesson is that it is important to detect overlapping dependencies from all Nth-parties in order to avoid concentration risk from an entity (or entities) in common with multiple Nth-parties.

Automation may be able to help for Nth-party identification. The heat map [2] shown in Figure 13 is an advanced visualization technique to help understand the complex and vast supply chain for a large hospital system. This heat map is an aggregation of all fourth-party suppliers to a hospital system under continuous monitoring. The fourth-party suppliers are grouped by cybersecurity ratings into different colors. The size of each rectangle is proportional to the percentage of market share for that supplier. By comparing heat maps from known 3rd- and 4th- party entities it may be possible to identify common N-th party entities to be forewarned of potential concentration risk from performance choke points and/or single-points-of-failure.

[2] A heat map (or heatmap) is a 2-dimensional data visualization technique that represents the magnitude of individual values within a dataset as a color. The variation in color may be by hue or intensity.

Figure 13. Fourth-Party Heat Map Grouped by Rating Scores [19]

Given that cybersecurity ratings are quantified numerical numbers, this provides an simple way to calculate TPRM return on investment (ROI). ROI can be measured in cybersecurity ratings changes given TPRM investments. For example, if an individual third-party cybersecurity rating (or an aggregate group of third-party cybersecurity ratings) is benchmarked and then there is a TPRM intervention, the ROI is the investment in dollars divided by the delta change in rating. In the case of a $1M TPRM investment for a ratings improvement change of 100 points the ROI would be one rating point increase per $10K investment. Intervention investments can then be strategically optimized, under a budget constraint, for evidence-driven strategic ROI cybersecurity TPRM decision-making.

VII. SUMMARY

An organization's security is only as strong as its weakest point. Attackers need just one entry point to bypass defenses, whether human error, vulnerable software, an insecure API, or a compromised third-party vendor. A strong security strategy must address and reinforce all potential vulnerabilities in people, processes, technology, and third-party relationships, as any weak link can compromise the entire system.

In this paper we focused on countering the growing threat of third-party cybersecurity risks with the establishment of structured third-party risk management (TPRM) programs to address this threat. Since there are different frameworks upon which to build a TPRM program and different internal TPRM processes we did not go into detail about TPRM mechanics, instead leaving that to the reader. However, we do provide a comprehensive list of references which do provide these third-party mechanics details [28-50].

Moving from reactive incident response to proactive third-party risk identification and proactive third-party continuous monitoring requires the use of automation. In this paper we emphasize the need for a TPRM program to use: (1) **automated quantifiable measurements for benchmarking and comparison** and (2) **automated dashboard tools to handle Nth-party scalability**. Automation is essential for organizational resilience in processing third-party information as supply chains grow exponentially larger and more complex.

Lastly, while we used explanatory examples in the healthcare context to illustrate points, the underlying concepts and practical techniques we shared are universal, certainly applicable to the third-party risk concerns of the Federal Reserve and the U.S. Banking industry as a whole.

ACKNOWLEDGMENTS

This work has been enabled through a cooperative agreement between the University of Illinois at Urbana-Champaign and BitSight. BitSight provided no financial support to this work. Cybersecurity ratings referenced in this work were processed by BitSight engineers led by Rhonda O'Kane and supported by Tadd Hopkins, Tim Jackson, Tom Linehan, and Will Ricardi. Geocoding was provided by GeoCoder.ca who provided public service access to their geography mapping scripts. Geocode provided no financial support to this research.

REFERENCES

[1] Peterson-KFF, "Health System Tracker," 2025. < https://www.healthsystemtracker.org/chart-collection/u-s-spending-healthcare-changed-time/>

[2] L. DePillis and C. Zhang,"How Healthcare Remade the U.S. Economy," NY Times, July 3 2025. <https://www.nytimes.com/interactive/2025/07/03/business/economy/healthcare-jobs.html >

[3] W. Haydock, "What is the Difference Between Supply Chain, Third-Party, and Vendor Risk Management?" Deploy Securely, Feb 10 2023. <https://blog.stackaware.com/p/what-is-the-difference-between-supply>

[4] J. Boyens, et. al., "Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations, " National Institute of Standards and Technology (NIST) NIST SP 800-161 Rev. 1 May 2022

[5] J. Licata, et. al., "Developing Security, Privacy, and Cybersecurity Supply Chain Risk Management Plans for Systems," National Institute of Standards and Technology (NIST) Initial Public Draft NIST SP 800-18r2 ipd June 2025.

[6] International Standards Organization (ISO) and International ElectroTechnical Commission (IEC), ISO/IEC 27036-1:2021, "Cybersecurity - Supplier Relationships - Part 1: Overview and Concepts (2nd edition)," 09-09-2021. <>

[7] International Standards Organization (ISO) and International ElectroTechnical Commission (IEC), ISO/IEC 27036-2:2022, "Cybersecurity - Supplier relationships - Part 2: Requirements (2nd edition)," 06-15-2022.

[8] International Standards Organization (ISO) and International ElectroTechnical Commission (IEC), ISO/IEC 27036-3:2023, "Cybersecurity - Supplier relationships - Part 3: Guidelines for Hardware, Software, and Services Supply Chain Security (2nd edition)," 06-13-2023.

[9] International Standards Organization (ISO) and International ElectroTechnical Commission (IEC), ISO/IEC 27036-4:2016, "Information Technology - Security Techniques - Information Security for Supplier Relationships - Part 4: Guidelines for Security of Cloud Services," 09-28-2016.

[10] Board of Governors of the Federal Reserve System, "Interagency Guidance on Third-Party Relationships: Risk Management," SR 23-4 June 7 2023.

[11] Third Party Risk Association (TPRA) "Third Party Risk Management 101 GuideBook (1st edition)," 2023. <https://www.tprassociation.org/>

[12] G.C. Rasner, "Cybersecurity & Third-Party Risk: Third Party Threat Hunting," Wiley 2021.

[13] G.C. Rasner, "Zero Trust and Third-Party Risk: Reduce the Blast Radius," Wiley 2024.

[14] W. Yurcik and A. Schick, "Preliminary Lessons from Change Healthcare Nationwide Pharmacy Supply Chain Failure," Fintech and Financial Institutions Research Conference (FinTech), April 2005. <https://www.philadelphiafed.org/calendar-of-events/fintech-and-financial-institutions-research-conference-2025>

[15] W. Yurcik, A. Schick, S. North, M.T. Gastner, F.R. Miranda; R.S. Avelino, A.F.M. Batista, G. Pluta and I. Brooks, "Cybersecurity Monitoring/Mapping of USA Healthcare (All Hospitals) – Magnified Vulnerability due to Shared IT Infrastructure, Market Concentration, &

Geographical Distribution," ACM CCS Workshop on Cybersecurity in Healthcare (HealthSec) 2024. <doi:10.1145/3689942.3694754>

[16] R. Anderson and T. Moore, "The Economics of Information Security," Science, Nov 2006.<doi: 10.1126/science.1130992>

[17] National Institute of Standards and Technology (NIST), "Measurement Guide for Information Security: Volume 1 – Identifying and Selecting Measures," NIST SP 800-55 Vol 1. January 17, 2024.

[18] W. Yurcik, S. North, R. O'Kane, O.S. Saydjari, F.R. Miranda, R.S. Avelino, and G. Pluta, "Measurability: Toward Integrating Metrics into Ratings for Scalable Proactive Cybersecurity Management," IARIA 19th Intl. Conf. on Emerging Security Information, Systems and Technologies (SECURWARE), 2025.

[19] W. Yurcik, R. O'Kane, S. North, O.S. Saydjari, F.R. Miranda, R.S. Avelino, R. Pluta, and G. Pluta, "Cybersecurity Risk Measurements of Rural Independent Under-Resourced Hospitals," Research Conference on Communications, Information and Internet (TPRC53) 2025.

[20] S.J. Choi and M.E. Johnson, "The Relationship Between Cybersecurity Ratings and the Risk of Hospital Data Breaches," J of the American Med Informatics Assoc. 28(10) 2021.

[21] "A Complete Guide to Third-Party Risk Management," UpGuard, 2023. <https://content.upguard.com/hubfs/resources/eBook%20-%20A%20Complete%20Guide%20to%20Third-Party%20Risk%20Management.pdf>

[22] M. Musser and D. Hulem, "GRF's Cybersecurity Guide: Risks and Mitigation Strategies," 2025.

[23] Black Kite Cyber Risk Platform, 2025. <https://blackkite.com/>

[24] Z. Amos, "How Cyberattacks Disrupt Healthcare Supply Chains," HealthIT Answers, Sept 16 2025. <https://www.healthitanswers.net/how-cyberattacks-disrupt-healthcare-supply-chains/>

[25] "5 Key Insights for Third-Party Risk Management Design and Governance," Gartner, 2024. <https://www.gartner.com/en/legal-compliance/topics/third-party-risk-management-tprm>

[26] G.R. Ledlow, K.B. Manrodt, and D.E. Schott, Health Care Supply Chain Management: Elements, Operations, and Strategies," Jones & Bartlett Learning, 2017.

[27] M.E. Porter and E.O. Tiesberg, "Redefining Health Care: Creating Value Based Competition on Results," Harvard Business School Press, 2006.

[28] T.O. Abrahams, et. al., "Reviewing Third-Party Risk Management: Best Practice in Accounting and Cybersecurity For Superannuation Organization," Finance & Accounting Research Journal 6(1) Jan 2024.

[29] BitSight, "A Security Manager's Guide to Third-Party Risk Management," White Paper, BitSight Technologies LLC. <https://www.bitsight.com/resources/security-managers-guide-to-third-party-risk-management>

[30] A. Cardwell, "Mastering Supply Chain Security in the Digital Age: A Comprehensive Guide to Safeguarding Interconnected Operations in Today's Cyber-Centric World," self-published 2025.

[31] A. Cardwell, "Mastering Third-Party Cybersecurity Risks," self-published May 2025.

[32] C. Crossley, "Software Supply Chain Security," O'Reilly 2024.

[33] S. Carnovale and S. Yeniyurt, "Cyber Security and Supply Chain Management: Risks, Challenges, and Solutions," World Scientific 2021.

[34] A. Dhongde, "Advanced Consepts of Risk Management and Resiliency in Supply Chain," self-published, 2025.

[35] A. Evans, A. Singh, and A. Golbin, "Navigating Supply Chain Cyber Risk," Routledge 2025.

[36] L.H. Harrington, S. Boyson, and T.M. Corsi, "X-SCRM: The New Science of X-treme Supply Chain Management," Taylor & Francis 2011.

[37] C. Hughes and T. Turner, "Software Transparency: Supply Chain Security in an Era of Software Driven Society," Wiley 2023.

[38] B. Johns, "Evolving Threats, Evolving Chains: Cybersecurity for the Modern Supply Chain," Penisula Network Security, 2025.

[39] O. Keskin, et. al., "Cyber Third-Party Risk Management: A Comparison of Non-Intrusive Risk Scoring Reports," Electronics 10 1168, 2021.

[40] J.K. Kwong and K. Pearlson, "Supply Chain Cybersecurity and Small and Medium-Sized Enterprises (SMEs): Exploring Shortcomings in Third-Party Risk Management of SMEs," 57th Hawaii Intl. Conf. on System Sciences 2024.

[41] G.S. Lynch, "Single Point of Failure: The Ten Essential Laws of Supply Chain Risk Management," Wiley 2009.

[42] J.B. de Melo, "Supply Chain Cybersecurity: The Beginner's Guide," self-published 2023.

[43] D.A. Olson, "Supply Chain Risk Management: Tools for Analysis (2nd edition)," Business Expert Press (BEP) 2011.

[44] Onetrust, "The Business Value of Third-Party Risk Management Software," onetrust, Dec2022. <https://www.onetrust.com/content/dam/onetrust/brand/content/asset/white-paper/ot-value-third-party-risk-management-software-white-paper/OT-value-third-party-risk-management-software-white-paper-US-digital.pdf>

[45] Onetrust, "InfoSec Guide to Third-Party Risk Management," onetrust, E-book, May 2023. <https://www.onetrust.com/content/dam/onetrust/brand/content/asset/ebook/ot-ultimate-guide-to-tprm-for-info-sec-ebook/OT-ultimate-guide-to-TPRM-for-info-sec-eBook.pdf>

[46] M.S. Pour, C. Nader, K. Friday, E. Bou-Harb, "A Comprehensive Survey of Recent Internet Measurement Techniques for Cyber Security," Computers & Security 128 2023. <doi:10.1016/j.cose.2023.103123>

[47] M.A. Russo, "21st Century Supply Chain Risk: SCRM 2.0," Cybersentinel 2021.

[48] "Third Party Risk Management Solutions," The Art of Service, August 2025.

[49] A. Wilson, "Supply Chain Security Management: The Key to Resilient and Secure Logistics," self-published 2024.

[50] S.A. Wright, "Securing Your Data Supply Chain Data Governance in the Digital Age," Macadamia Solutions 2024.