BRC
BOARD RISK COMMITTEE
BOARD RISK REPORT

February 29, 2024

CYBER RISK IN THE CONTEXT OF VENDOR RISK MANAGEMENT
Is Your Board Prepared for Evolving Complexity and Increased Regulation?

By Lynn Terwoerds

Boards of directors have seen cyber security third-party risk management evolve into a multi-layered, increasingly complex interconnected global concern, but not all boards recognize this new reality.

As recently as late 2021, the influential Bank Policy Institute (representing more than forty of the nation's leading banks), responding to a request for comments on updated integrated OCC/FRB/FDIC guidance, stated:

> *"...board[s] of directors should be expected to review, discuss, and approve overall risk management strategy for the banking organization and oversee the establishment of policies, but the policies that are to be approved by the board of directors should be limited to the most important ones (e.g., the banking organization's capital policy). Approval of the vast majority of policies that address day-to-day operations — including, for many banking organizations, the third-party risk management policy — should be within the sole purview of senior management, which has the subject matter expertise, experience, and time to perform this role effectively." [1]*

In its final release, regulators maintained the requirement for boards of directors' oversight for third-party risk management, and for good reason. Without strong board oversight of vendor risk management programs, the enterprise will be at a distinct disadvantage as evolving technologies confront the entire supply chain. Consider the recent example of a new security protocol added to Apple's iMessage service in preparation for the coming quantum computing environment. This change to existing supply chain hygiene exemplifies the proper forward looking perspective so critical to protecting organizational assets in a fast arriving future [2].

This *Board Risk Report* will examine three driving forces so boards can better prepare for the evolving complexity and increased regulation of cyber risk in the context of vendor risk management.

THE EVOLUTION OF THIRD-PARTY CYBER RISK

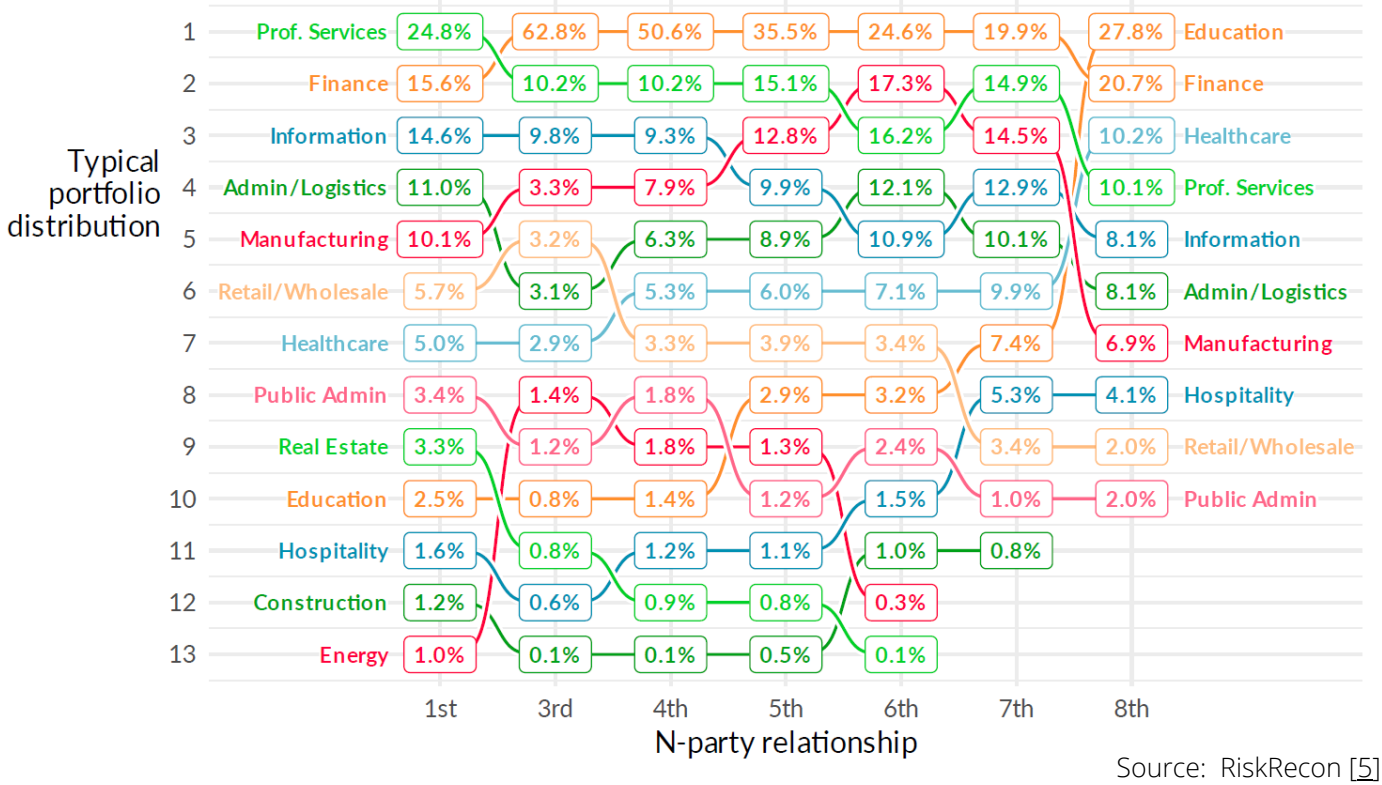
Enterprise vendor risk is hardly a new topic for board risk committees. For years companies have turned to third parties for important business reasons such as faster access to innovation, leveraging economic models of new tech, digital transformation, and other paths that lead to competitive advantage and efficiency. At the same time, there has been a dramatic rise in cyber breaches originating from widely used vendors such as SolarWinds [3] and MOVEit [4]. Both were catastrophic events because these vendors were part of a widely used worldwide supply chain and put millions of people and company data at risk. The SolarWinds breach was reported in December 2020 and in October 2023 the SEC filed charges against SolarWinds and its CISO for defrauding investors among other serious charges. It was also the first time the

SEC brought cybersecurity enforcement actions against an individual.

Vendor risk management is a well-established discipline with organizations such as Shared Assessments providing conferences, blogs, papers, certifications, and research in the face of a rapidly evolving risk environment. Many, but not all, boards are aware of interrelated driving forces making vendor cyber risk management more challenging:

1. **Complexity** – Modern enterprises are sprawling digital estates with interconnected and interdependent technologies. You own some parts and vendors manage others. There are separate and shared responsibilities, an increasingly complex supply chain composed of a multitude of contractual agreements and a lifecycle that should support evolving strategic business goals. Threat actors know this is a weakness. A good primer on increasingly complex supply chains is the recently published, "Risk to the Nth Party Degree" which discusses the network of dependencies that make up the vendor landscape of today and the ever-expanding challenges to manage it [5]. Some of the largest recent breaches prove aggressors don't even need to attack their targets directly.

Typical Distribution of Industries Across an Organizational Supply Chain



Source: RiskRecon [5]

2. **Regulation** – Regulators in the EU, UK, US, and other jurisdictions have demonstrated concern over TPRM and the interdependencies of supply chains that impact businesses, markets, and infrastructures globally. Risk committees have an obligation to ask probing questions about their entire business ecosystem and risks associated with 4th and 5th party risk.

3. **Weak Incident Response** – Vendor incident response plans have been stress tested and there have been some very visible failures. For example, a US government agency and two cybersecurity companies advised SolarWinds of security breaches well before the company disclosed in December 2020. SolarWinds also knew of security vulnerabilities in the platform a month beforehand. Progressive Software, maker of MOVEit, learned the lesson and responded quickly in 2023 [6].

I believe focusing on the business and governance will help directors navigate these intricate times. Considering the three driving forces mentioned above, directors can begin to tackle the evolving complexity while focusing on these three key areas:

1. **Manage Complexity with Business Acumen**
   Of course, directors should avoid getting into the weeds. When managing technology risk concentrate on the realities of today's extended enterprise and acknowledge that vendors are part of critical business processes and often handle and store sensitive data. Focusing on the complete infrastructure hygiene that supports the business and business strategy is tantamount for directors.

   Critical Questions Directors Should Ask:
   - Does the third-party risk management program (which must deal with important risks across almost all risk domains) function as a key component of your organization's enterprise risk management program?
   - How does your organization's cyber risk management program support vendor risk management activities, including continuous monitoring and supply chain documentation?
   - Are the Chief Risk Officer, Chief information Security Officer, Chief Information Officer, and the Chief Technology Officer all on the same page in terms of future vendor program management direction?
   - How operationally efficient is your TPRM program? Does the board mandate periodic, arm's length reviews of your vendor risk management program?
   - When new vendors are selected, does appropriate due diligence confirm that these firms can meet your internal operational and financial hygiene requirements?
   - Has your CRO recently raised resource concerns to your risk or audit committee? Have you invested in the right people? Given new regulations, directors should ask management again whether the company is properly invested in TPRM.

2. **Regulatory Impact**
   Recent regulations, whether the SEC final cybersecurity rule, The EU's Digital Operational Resilience Act (DORA) or UK's CP 26/23, have new requirements and guidance for vendor risk management. Regulators around the world are updating third-party risk management regulations:

   - **January 2023** – DORA [7] is EU regulation for the financial sector, broadly defined [8]. Third-party supply chain risk is a key area of focus and ICT (Information and Communication Technology) third-party suppliers are explicitly covered by the Act.
   - **April 2023** – The Canadian Supervisor of Financial Institutions issued new vendor risk management guidance requiring firms to consider the use of subcontractors and the complexity of its supply chain when determining the degree of risk a vendor presents to the outsourcer.
   - **July 2023** – The SEC adopted new rules for public companies in the areas of cybersecurity risk management, strategy, governance, and incidents. The SEC cybersecurity rule requires companies under their jurisdiction to disclose whether they have "processes to oversee and identify such risks from cybersecurity threats associated with its use of any third-party service provider."
   - **December 2023** – The Bank of England published consultation paper CP 26/23 outlining requirements and expectations for critical third parties. It recognizes the impact critical third parties have on financial stability and financial markets worldwide and has a strong focus on supply chain risk management.

Directors Should Consider the Following:

- When was the last time the board and corporate counsel reviewed the vendor risk management policy? Do the minutes reflect any probing questions from directors?
- How often does the risk committee or board get a CRO briefing? Does the CRO provide updates on:
    - Mandatory cybersecurity practices for all vendors. How is adherence to such practices confirmed?
    - Does your organization have appropriate critical third-party risk management processes and reporting metrics in place?
    - How does your firm handle the inherent friction between onboarding a critical vendor and finishing the due diligence process? While business needs may require fast onboarding, does the executive team ever justify a hurried or incomplete due diligence process for a business critical or high-risk vendor?
    - Have contracts and master services agreements been properly reviewed? Are there legacy contracts that need updating to reflect common practices such as multi-factor authentication? Is the contract lifecycle in sync with business needs and the changing threat landscape?
    - How does executive management keep up with changes in vendor security posture, exposure to new vulnerabilities, ecosystem risks from 4th and 5th parties, etc.?

3. **Incident Response Issues**

Under the new SEC cybersecurity rule, directors have responsibility to know when there's been a material breach [9]. If your vendor has a breach that materially affects your business, your firm will be required to report the incident. There are reporting requirements and an 8-K filing process that I won't cover in detail here but will address the most pressing questions directors should ask:

- In preparation for compliance with the SEC cybersecurity rule, has executive management and legal counsel undertaken the steps to enumerate what is material? No one can predict when a cyber incident will occur but enumerating what is material is doable and will save time during a crisis.
- How soon will board members be alerted to a material cyber event? Has that alert process been tested, especially if it is new? While the SEC has a four-business day timeline to report, there is sufficient flexibility for boards and management to consider accuracy as well as timing. IBM says it takes 277 days on average to identify and contain a breach [10]. Boards should understand the internal process leading to a decision that a true incident has occurred for reporting purposes, including the organization's definition of "materiality." Boards should be informed as soon as management suspects a cybersecurity event may rise to the level of a reportable incident.
- Directors may also want to inquire what incident response frameworks are being used and their relevance to the business. Examples include the NIST Cyber Security Framework (CSF) or the Bank of England's Prudential Regulation Authority (PRA) requirements [11]. NIST provides core functions for incident response, while Bank of England provides requirements for UK financial institutions reporting material incidents that could result in serious disruption, loss or reputational damage. The Bank of England's proposal outlines a requirement for at least three reports for each incident cycle [12].
- When (and how often) was the latest test of the security incident response plan? What were the gaps and lessons learned? The obvious lesson is to practice and be prepared beforehand.

REFERENCES:

[1] https://bpi.com/about-us/

[2] https://brianlenahan.substack.com/p/the-apple-imessage-impact

[3] Recent discussion of the SolarWinds fallout: https://www.forbes.com/sites/stewartroom/2023/11/01/solarwinds-is-a-game-changeryou-cannot-sugarcoat-cybersecurity/?sh=400be0dd62cb

[4] A good article on the still unknown scope of the MOVEit breach: https://www.wired.com/story/moveit-breach-victims/

[5] Report: Risk to the Nth Party Degree https://www.riskrecon.com/report-risk-to-the-nth-party-degree#:~:text=In%20this%20new%20study%2C%20we,parts%20of%20your%20supply%20chain

[6] https://www.rapid7.com/blog/post/2023/06/14/etr-cve-2023-34362-moveit-vulnerability-timeline-of-events/

[7] The regulation - https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2554. A KPMG blog discussion https://kpmg.com/lu/en/blogs/home/posts/2023/04/dora-regulation-all-your-questions-answered.html.

[8] This Regulation applies to the following entities: (a) credit institutions, (b) payment institutions, (c) electronic money institutions, (d) investment firms, (e) crypto-asset service providers, issuers of crypto-assets, issuers of asset referenced tokens and issuers of significant asset-referenced tokens, (f) central securities depositories, EN 29 EN (g) central counterparties, (h) trading venues, (i) trade repositories, (j) managers of alternative investment funds, (k) management companies, (l) data reporting service providers, (m) insurance and reinsurance undertakings, (n) insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries, (o) institutions for occupational retirement pensions, (p) credit rating agencies, (q) statutory auditors and audit firms, (r) administrators of critical benchmarks, (s) crowdfunding service providers, (t) securitization repositories, (u) ICT third-party service providers

[9] The definition of materiality is consistent with materiality under securities laws, i.e., materiality is defined as “substantial likelihood that a reasonable shareholder would consider it important in making an investment decision” or it would have “significantly altered the total mix of information made available.” See: Final Rule: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure: https://www.sec.gov/files/rules/final/2023/33-11216.pdf

[10] https://www.ibm.com/reports/data-breach-action-guide#:~:text=It%20takes%20277%20days%20on,deploy%20in%20just%202%20years

[11] NIST CSF core functions: Identify, Protect, Detect, Respond, Recover. PRA requirements: Scope/impact, Criteria/loss, disruption, reputation, Process/report through appropriate channels.

[12] See: CP26/23 - Operational resilience: Critical third parties to the UK financial sector | Bank of England, sections 7.8 – 7.19, https://www.bankofengland.co.uk/prudential-regulation/publication/2023/december/operational-resilience-critical-third-parties-to-the-uk-financial-sector

ABOUT THE AUTHOR

Lynn Terwoerds

Ms. Terwoerds serves as an independent director on the board of First Fed (FNWB) where she is on the Audit & Risk, Fintech, and Asset & Loan Quality committees. She is also the current board chair of the Northwest Maritime Center (nonprofit) and on the advisory board of the Executive Women's Forum.

For more than 25 years, Ms. Terwoerds has been an outstanding technology thought leader and cybersecurity risk strategist for very large global companies – Microsoft, Barclays PLC, Oracle Corp. Lynn's background includes senior leadership positions in multiple vertical markets ranging from technology to banking and healthcare. She is also a founding member of the Cloud Security Alliance.

Lynn graduated with a Master's degree in Classics from the University of Missouri-Columbia and holds a Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), National Association of Corporate Directors (NACD) Directorship Certification™.

UPCOMING EVENT

Geopolitical Risk Here and Abroad
Speaker: The Honorable Deborah K. Jones, US Ambassador (ret)
Wednesday, March 13, 2024
11:00 AM – 12:00 PM ET, *1-Hour Webinar*

**Complimentary to attend - Registration is Required*

Register - Mar. 13

JOIN THE BRC - MEMBERSHIP OPPORTUNITIES

INDIVIDUAL MEMBERSHIP - Special $200 Rate - NOW through June 30, 2024
Click here to learn more about membership and join online today.

CORPORATE BOARD MEMBERSHIP PROGRAM - $1,500 Annual Rate - up to 7 Individual Members
Click here to learn more - Contact Susan C. Keating to join today: susan@boardriskcommittee.org

CONSULTING SERVICES
Click here to learn more - Contact Susan C. Keating to get started: susan@boardriskcommittee.org

WHO WE ARE: The Board Risk Committee (BRC) is one of the foremost thought leadership peer councils for board risk committee members and chief risk officers. The BRC is a nonprofit, non-competitive, trusted place for the exchange of ideas, strategies, and best practices in enterprise risk oversight. We advocate for having risk committees of boards, where appropriate, and for educating board directors about enterprise risk. The BRC aims to foster more effective risk management and board oversight. The BRC works in partnership with The Santa Fe Group (SFG) and Shared Assessments (SA). SFG is a strategic advisory company providing expertise to leading corporations and other critical infrastructure organizations in the area of risk management. SA is a member-driven organization that provides thought leadership, products, education, and certifications in the third party risk management space. *The Board Risk Report is the periodic publication of the BRC.*

BRC Contacts: Catherine A. Allen, Founder and Chair of the Board, cathy@boardriskcommittee.org; Ellen Dube, Executive Director, ellen@boardriskcommittee.org; Susan C. Keating, Chief Partnership Officer, susan@boardriskcommittee.org