Third Party Risk Management:

Just the Right Thing to Do

LYNX TECHNOLOGY PARTNERS

NTSC
NATIONAL TECHNOLOGY SECURITY COALITION

More About the Author

Angela Dogan is Director of Vendor Risk & Compliance Services at Lynx Technology Partners. Prior to Lynx, she spent the last 14 years working in the financial services industry. Angela has a vast array of knowledge in information security, vendor risk management, and executive level client relations. Her expertise is in implementation and execution of third-party risk management programs.

Angela is an active member of the Cloud Security Alliance CCM Working Group where she was one of six who won the 2018 Ron Knode Service Award. This award is given to volunteers for their dedication and efforts to furthering cloud security best practices.

By Angela Dogan

Lynx Technology Partners
Director of Vendor Risk & Compliance Services

More About the Author

Kevin Howarth is a senior cyber writer and content marketing consultant with the National Technology Security Coalition. His background includes more than 15 years of information technology and cybersecurity writing, editing, and content marketing focused on C-level and senior technology leaders. With experience in B2B copywriting, magazine editing, business development, and content strategy, Kevin has helped build the NTSC's content marketing strategy while generating timely, regular, relevant content for its audience of CISOs, national policymakers, and other cybersecurity stakeholders.

By Kevin Howarth

National Technology Security Coalition
Content Strategy and Marketing Consultant

With scrutiny on companies intensifying as data breaches become a matter of when, not if, the subject of Third Party Risk Management (TPRM) enters the cybersecurity spotlight more and more. A November 2018 Opus and Ponemon Institute study noted "59 percent of companies said they have experienced a data breach caused by one of their vendors or third parties. In the U.S., that percentage is even higher at 61 percent – up 5 percent over last year's study and a 12 percent increase since 2016." Yet, despite this reality, a July 2018 CrowdStrike report notes "fewer than a third (32 percent) of respondents' organizations have vetted all of their suppliers, new or existing, over the past 12 months."

What's going on here? If a data breach is a third party's fault, companies still receive the blame. Yet, companies fail to create TPRM programs—or implement them properly—even as data breaches increase in quantity and severity. Especially in less regulated industries, many organizations do not have mature TPRM programs. Even larger companies struggle with the volume and complexity of thousands of third-party vendors.

The absence of mature TPRM programs does not result from a lack of available best practices. Plenty of resources exist that cover:

- Assessing risk (inventorying and evaluating vendors).
- Managing risk (creating processes, procedures, policies, contracts, and SLAs).
- Working with third-party vendors (due diligence, continuous assessments, communication, collaboration).
- Independently assessing risk with external frameworks (NIST 800-53, ISO 27001/2, Shared Assessments Program, Cloud Security Alliance Cloud Controls Matrix).
- Planning for worst-case scenarios (incident response, data breach notification, alternate options in case something bad happens to a vendor).

Reiterating the same best practices will not address the obstacles preventing organizations from maturing their TPRM programs. In this whitepaper, we want to explore the obstacles to TPRM maturity, offer recommendations that will help organizations get past those obstacles, and explore how legislation, regulations, and standards are helping organizations adopt stronger TPRM programs.

Specifically, this whitepaper will examine:

1. Why more TPRM programs are not mature and what unique obstacles make risk management programs challenging for even large companies.
2. What a mature program looks like, who owns risk management, and how different departments need to work together.
3. How legislation, regulations, and standards help promote the adoption of mature TPRM programs across all organizations.

Obstacles to TPRM Maturity

Many organizations have no formalized TPRM program and, at the core, lack an understanding about how to analyze their risk posture. The two main questions we hear from organizations are "Where do we start?" and "How do we start?" These are difficult questions to answer for organizations that suffer from the following struggles:

- **Low board and executive leadership support and participation**. The 2019 Vendor Risk Management Benchmark Study: Running Hard to Stay in Place, sponsored by the Shared Assessments Program and Protiviti, shows that organizations with high levels of board engagement have more mature TPRM programs. Conversely, organizations with low board engagement are three times more likely to have either ad hoc TPRM programs or no program at all. This tells us that a major key to having a mature TPRM program is the tone at the top. If boards and executive leadership are engaged in the building of a TPRM program, organizations will have a greater ability to build mature, successful programs.

- **Inability to find the right people or lacking budget for resources**. With the impact of laws and regulations on organizations that affect managing the security of third-party assets combined with the increased number of outsourced products and services, organizations find it more and more difficult to identify people who understand third-party risk. Often, people are pulled from other areas of an organization to lead or create TPRM programs who have no clear knowledge of how to do so. This situation results from organizations not having budgets allocated to TPRM programs. The Shared Assessments Program Vendor Risk Management Benchmark Study found that 36 percent of organizations rated their capabilities for the allocation and optimization of resources well below the target level.

- **Substituting tools for inexperience when establishing a TPRM program**. As mentioned in the previous bullet, resources are often pulled from other areas of an organization to create and implement TPRM programs. As a result, the program head is inexperienced in understanding the elements that make for a mature program. That's why many organizations get sold on the notion that a "tool" is the end-all and be-all to managing and successfully maintaining TPRM. While tools can offer greater process efficiencies, an organization must lay a mature foundation before any tool can succeed.

Because of financial services industry regulations and standards, it is commonly known that many large financial services industry organizations are considered very mature in the TPRM space. However, the Shared Assessments Program Vendor Risk Management Benchmark Study noted in 2017 that on a maturity level range of 1 to 5 (with 5 as most mature), the financial services industry ranked around 3.3. This tells us that even the most regulated industry has TPRM program maturity issues—and the problem continues today.

Through our experience, we've witnessed a few problems and areas of opportunity for larger organizations with TPRM programs that are similar to organizations without a mature program. Some of those major problems include:

- **A lack of a TPRM program foundation truly based on the risk factors of the organization**. The most difficult TPRM question today is, "How do we determine, assess, and quantify risks?" Unfortunately, no magic formula or cookie cutter method exists, and each organization's risk factors may differ. Larger organizations tried to solve this problem by purchasing Governance, Risk Management and Compliance (GRC) tools and platforms—and yet they still struggle because a good TPRM program foundation was not laid in the beginning.

- A **large volume of third-party vendors**. Some large companies can work with thousands or even tens of thousands of third-party suppliers globally. They struggle with vendor inventory as well as data inventory. Those struggles equate to the struggle of managing data security effectively. Even the most experienced CISO struggles to oversee security under these conditions.

- **Poor due diligence**: Information security within the due diligence process has been difficult for many organizations, especially during mergers and acquisitions. Often, companies get acquired without much thought by the acquirer about assessing their information security practices and controls. This results in issues identified after the deal finalizes.

- **Issues with processes**: Many organizations struggle with a lack of truly "risk-based" processes. They have implemented checklist-type assessments that lack any real analysis of the risk impacts presented by third parties. This may include only a review of their high-risk vendors identified as high-risk because of the impact to an organization's financials. True risk-based TPRM programs include several factors that make up these risks and a tiering of an organization's entire third-party inventory based on those factors. Mature TPRM programs also incorporate continuous monitoring, which consists of periodic assessments and analysis of data that's available on their third parties.

- **Unique, evolving, and innovative technologies**: The third-party supply chain attack surface continues to increase with more cloud, IoT, AI, and blockchain vendors. Because many of these technologies do not require traditional hardware and software that an IT team would oversee, it's easy to overlook the security risks when purchasing such solutions that require little to no deployment or installation time.

Whether an organization does not have a foundation in place or struggles with the overwhelming complexity of modern TPRM for thousands of vendors, the same solution beckons: taking the time to develop a risk-based TPRM program foundation.

Mature TPRM Programs

Every company is different, and no clear-cut or cookie cutter TPRM formula exists that applies to all organizations. However, a few elements make some TPRM programs more mature than others. Based on the Shared Assessments Program Vendor Risk Management Maturity Model (VRMMM), We will identify the eight elements that make up a solid TPRM program based on cross-industry best practices.

1. Program Governance
2. Policies, Standards, and Procedures
3. Contracts
4. Vendor Risk Identification and Analysis
5. Skills and Expertise
6. Communication and Information Sharing
7. Tools, Measurement, and Analysis
8. Monitoring and Review

Program Governance

A good TPRM program starts with formalized objectives and board oversight that will provide structure and standards of conduct. Here, you also show alignment with whatever industry standard your organization has chosen (such as ISO 27001/27002 or NIST 800-53 rev 5). Program governance also houses your program's organizational structure. A lot of debate continues about where a TPRM program should operate within an organization, but it really depends on the organization. The most important thing to keep in mind as an organization makes this determination is that a good TPRM program operates independently. Whether an arm under the CISO, CRO, or COO, it must have defined criteria that ensures independence.

Policies, Standards, and Procedures

Policies and procedures are always an indicator of a mature program because they form the program's foundation. Clearly defined policies and procedures regarding TPRM, inventory requirements, vendor classification, contract management, and vendor termination / exit procedures are critical to a successful TPRM program and need definition.

Contracts

A defined organizational structure for third-party contract drafting is a critical element of any TPRM program. A lack of certain mandates such as the right to audit, SLAs, security requirements, and key risk indicators are detrimental to the success of the program. Often, these mandates are only considered after a signed contract but it is important to consider them as common practice for every contract from the beginning.

Vendor Risk Assessment Process

Here, working with various lines of business is critical because you want to make sure you define business requirements for outsourcing by defining and assessing risk for the organization as a whole as well as for each line of business. You also want to make sure you structure a risk-based approach to TPRM which includes determining your risk factors for the organization, risk-ranking your vendors, and developing criteria for the risk categories. Then, you want to determine what your reporting will encompass by answering the question, "What would senior management and the board want to see?" Finally, you develop a plan for automation and how to implement it.

Skills and Expertise

This is a critical element because having the right people within your program can really impact its success. You want to make sure you define roles, responsibilities, competencies, and training programs along with developing a mechanism for determining staffing level needs and making sure you have the budget resources.

Communication and Information Sharing

How your TPRM program will integrate with other areas such as procurement, legal, and business units must be defined, implemented, and communicated as well as approved by senior management. It is important to make sure you have created processes for periodic reporting to the various areas of your organization that will have an impact on the program's success. Lastly, develop a process for how you will communicate and handle vendor assessment results. Who will own the risk? How will the risk be mitigated? What are your escalation procedures? The answers to these questions indicates the maturity of your TPRM program.

Tools, Measurement, and Analysis

This area is all about program management. It includes processes related to workflow management, risk scoring, and vendor assessment along with who is engaged in the process within the organization and how they are engaged. It also outlines what reporting, measurement, and analysis tools should be in place for continuous monitoring of the program. A mature TPRM program uses an objective, risk-based approach to TPRM, so you want to make sure those foundational elements are considered as you lay the foundation of the overall program.

Monitoring and Review

Continuous monitoring is a mandate for organizations operating in the financial services industry, but it is also just the right thing to do for any industry. Monitoring your third parties from a risk perspective is critical to the success of the organization. Remember, it is not if but when your organization will be breached. You want to make sure your program includes monitoring and review processes for contracts, SLAs, data security, and operational processes.

Legislation, Regulations, and Standards Point to Increased TPRM Importance

Several industries have governmental guidance and requirements related to TPRM. A few examples are listed below along with an overview of how these industries are impacted:

- **Financial services:** The financial services industry is required to follow a host of regulations as detailed by the Securities Industry and Financial Markets Association (SIFMA). Regulatory requirements have so critically impacted this industry that several groups such as the Financial Services - Information Sharing and Analysis Center (FS-ISAC), the Shared Assessments Program, and SIFMA have formed over the years to offer guidance on how to comply.

- **Healthcare**: The healthcare industry is a roaring second with industry regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act which focus on TPRM and data privacy.

- **Public companies:** The Sarbanes Oxley Act (SOX) touches on TPRM in its public company requirements.

- **Government**: The Federal Information Security Management Act (FISMA) applies to all government information—including information handled by third parties.

- **Education**: The Family Educational Rights and Privacy Act of 1974 (FERPA) applies to education information handled by third parties.

- **Payment card transactions:** The Payment Card Industry Data Security Standard (PCI DSS) applies to any business handling payment card information—a common third-party security vulnerability.

- **Energy**: The Federal Energy Regulatory Commission (FERC) has been more aggressively creating standards related to supply chain cybersecurity.

Data breach notification laws in each state also indirectly encourage a strong TPRM program because, even if a data breach is the fault of a third-party supplier, the company is still to blame. The Federal Trade Commission continues to enforce breaches and lapses in TPRM. According to a case in its 2018 annual report, "The FTC alleged that mobile phone manufacturer BLU Products, Inc. and its co-owner allowed a China-based third-party service provider to collect detailed personal information about consumers, such as text message contents, which the service provider did not need, and which were contrary to promises BLU made to consumers. As part of the settlement, defendants must implement a comprehensive data security program to help prevent unauthorized access to consumers' personal information and address security risks related to BLU phones. In addition, BLU will be subject to third-party assessments of its security program every two years for 20 years."

Though most federal laws that have been implemented relate to governmental bodies, a couple of laws have focused on the private sector such as S.29 (A bill to establish the Office of Critical Technologies and Security). According to CSO Online, "Senator Mark Warner (D-VA) introduced this bill early in the new Congress. A companion bill in the House, sponsored by Representative Dutch Ruppersberger (D-MD) H.R. 681, quickly followed. The legislation proposes a new 'Office of Critical Technology and Security' to coordinate technology supply chain security efforts. The office, which would report to the President, would be assigned the task of stopping 'the transfer of critical emerging, foundational, and dual-use technologies to countries that pose a national security risk' and developing a 'strategy to inform the private sector about critical supply chain risks.'"

S.29 shows a cooperative interest in reducing supply chain risk. In 2018, DHS attempted to engage more with the private sector concerning TPRM. Under DHS's Cybersecurity and Infrastructure Security Agency (CISA), its National Risk Management Center created the Information and Communications Technology (ICT) Supply Chain Task Force—a "public-private partnership to act as the federal focal point to examine and develop consensus recommendations to identify and manage risk to the global ICT supply chain."

Started in 2008, NIST's Cyber Supply Chain Risk Management (C-SCRM) program specifically addresses a critical infrastructure organization's risk management process and supply chain visibility with a set of standards allowing for flexibility and customization. The April 2018 update to the voluntary NIST Cybersecurity Framework Version 1.1 expanded upon and highlighted C-SCRM more within its guidelines. A new category states that, if successful, "the organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks." Five subcategories elaborate upon what makes this goal achievable.

Additional NIST publications such as Special Publication 800-53 (Revision 4 and Draft Revision 5), Special Publication 800-161: Supply Chain Risk Management Practices for Federal Information Systems and Organizations, and Special Publication 800-171 also continue to heavily influence the private sector. From the Fourth Revision onward, NIST 800-53 specifically includes supply chain security as part of the required security controls for federal agencies—with NIST 800-161 delving deeper into this topic. And the DoD continues to prioritize TPRM through recent revisions to NIST 800-171 and encourage heightened awareness about supply chain vulnerabilities that threaten national security.

Fortunately, global standards exist that the private sector utilizes such as the ISO 27000 series, Shared Assessments, and the Cloud Security Alliance (CSA). The influential Shared Assessments Program has developed a set of standards based on several cross-industry standards and best practices. They have also developed two certification programs with the goal of impacting the quality of TPRM program employees—the Certified Third Party Risk Professional (CTPRP) and the Certified Third Party Risk Assessor (CTPRA) certifications.

The Cloud Security Alliance's Cloud Controls Matrix (CCM) also helps provide standards around third-party cloud security vendors. As summarized in a joint NTSC/CSA whitepaper, "The CSA CCM provides both cloud providers and customers with needed structure, detail, and clarity relating to information security. The CCM provides fundamental cloud control objectives around three key areas: cloud architecture, cloud governance, and cloud operations. It also includes context around cloud provider versus customer control responsibilities as well as mappings to popular standards such as PCI/DSS, ISO/IEC 27001, COBIT, NIST 800-53, and many more. Used by enterprises as the controls framework baseline for their transition to cloud computing, the CCM is typically mapped against the internal information security management system (ISMS)."

All together, existing industry regulations alongside voluntary yet widely adopted standards such as NIST continue to help companies. It's clear that TPRM is being addressed across various industries in both the public and private sectors by helping companies develop a roadmap and providing confirmation of the right things to do. In today's modern threat landscape, unregulated companies should regulate themselves because it is the right thing to do. Lack of a TPRM program can cost an organization money, its reputation, and its survival.

Conclusion

The expensive aftermath of a data breach, the investigative authority of the FTC, and competitive benchmarking should serve as a fear-based incentive. Beyond fear, as we've mentioned several times, TPRM is simply the right thing to do. It secures your company's data, protects customers, and promotes cybersecurity best practices across the supply chain. As we often say in the cybersecurity industry, compliance alone does not necessarily equal security—taking companies as far as the law or regulation mandates and no more. The days of checklists won't suffice in the reality of the modern threat landscape.

If organizations are not addressing TPRM head on, they should. Any industry that deals with consumer information should hold themselves to a high standard. We as an industry must continue leading in this area while using federal regulations and cross-industry standards as guidance and foundational elements. With the support of organizations such as the National Technology Security Coalition that continue to bring the CISO's voice to Washington, D.C. with the goal of impacting the way lawmakers, regulators, and policymakers see TPRM, all industries will begin to understand and accept that building mature TPRM programs is just the right thing to do.

About the National Technology Security Coalition (NTSC)

The National Technology Security Coalition (NTSC) is a non-profit, non-partisan organization that serves as the preeminent advocacy voice for Chief Information Security Officers (CISOs) across the nation.

Through dialogue, education, and government relations, we unite both public and private sector stakeholders around policies that improve national cybersecurity standards and awareness.

Twitter @NTSC_CISO

NTSC
NATIONAL TECHNOLOGY SECURITY COALITION

About Lynx Technology Partners

Lynx Technology Partners is the trusted Information Security and Risk Management Advisor that customers in highly-regulated industries worldwide depend on to improve security posture, facilitate compliance, reduce risk, and refine operational efficiency. With world-class skills and knowledge capital built over 30 years, Lynx security experts help customers recognize and control IT-related risks and maintain compliance with major industry and government standards. Through consulting, security and risk assessments, penetration testing, managed security services, cyber ranges and immersive training, and an award-winning GRC solution, Lynx supports many critical projects for security-conscious leaders in Financial Services, Federal, Energy, Healthcare, State Government, and Higher Education.

For more information, please visit LynxRiskSolutions.com.

LYNX
TECHNOLOGY PARTNERS