sia partners

INSIGHT
September
2020

Managing Cybersecurity Risk Posed by Third Parties

Best practices to reap the benefits of outsourcing to third party vendors while defending against cyber threats

Understanding and addressing the cybersecurity risks posed by third parties has never been more important than now as modern organizations are increasingly outsourcing their business functions. Even with robust internal cybersecurity standards, it is impossible for organizations to ensure they are adequately protected against third party cybersecurity threats without a sophisticated Third Party Risk Management (TPRM) program. Due to the growing number of cybersecurity attacks via third parties in recent years, there is an urgent need for organizations to scrutinize the cybersecurity risks posed by the third party vendors they engage with.

Third Party Cybersecurity Risk

Third party risk arises from a firm's dependence on outside parties to perform activities or provide services on its behalf. This risk is measured against the likelihood (and resulting impact) that an outside party is unable to provide the activities/services required to support a firm's business or security needs. There are several common risks associated with third party vendors, one of which includes the risk of exposing internal company data to outside threats via third parties, otherwise known as third party cybersecurity risk. As organizations engage third parties to assist with various facets of their business, their once separate digital environments become increasingly connected, significantly expanding the potential attack surface to cyber predators.

In recent years, there have been numerous cybersecurity attacks on organizations by third parties. The cybersecurity attacks on financial services firms via the third party messaging system, SWIFT, serve as prime examples of why good TPRM cybersecurity practices are so important. One of the biggest attacks involving SWIFT-using banks was against the central bank of Bangladesh, who ended up losing $81 million as a result. While SWIFT was designed to ensure that money-moving messages between financial institutions are legitimate, the attackers injected fraudulent messages into the third party messaging system, ultimately moving money into accounts controlled by the attackers. Subsequent investigations into these cybersecurity attacks involving SWIFT showed that the attackers performed a considerable amount of research on their targets, and their vulnerability to a breach through the third party messaging system, prior to launching their attack[1]. Having a robust TPRM program in place can significantly decrease the likelihood of an event like this occurring at your firm. This paper will provide guidance and discuss best practices in order to ensure your business has a strong TPRM program in place to protect against cybersecurity threats.

OCC's Recent TPRM Cybersecurity Guidance

One of the most relevant and notable recent pieces of regulatory guidance related to TPRM cybersecurity came from the Office of the Comptroller of the Currency (OCC) on June 29th, 2020 via their Spring 2020 Semiannual Risk Perspective report[2]. This report addresses the most pressing issues and threats currently facing banks, specifically focusing on the impact of the COVID-19 pandemic on the federal banking industry. In this publication, the OCC stresses the necessity for banks to actively monitor and assess the increased cybersecurity and operational risks that have resulted from their implementation of new business systems and processes in response to the COVID-19 pandemic, especially when engaging third parties to assist in these efforts.

The OCC states, "Cyber threat actors continue to target banks, their customers, and their third parties. These threats continue to adapt and elevate due to increased criminal activity and sophistication. Phishing threats against bank customers and staff are elevated, and there have been an increasing number of attacks focused on the use of virtual private networks, virtual teleconferencing services, and other remote telecommunication technologies because of widespread transitions to telework models."

The OCC also notes that most banks successfully enacted business continuity plans and engaged third parties to support various facets of their operations in response to the COVID-19 pandemic. While these new business processes and third parties allowed for banks to maintain their routine operations during abnormal times, they also presented the following new operational risks and control considerations:

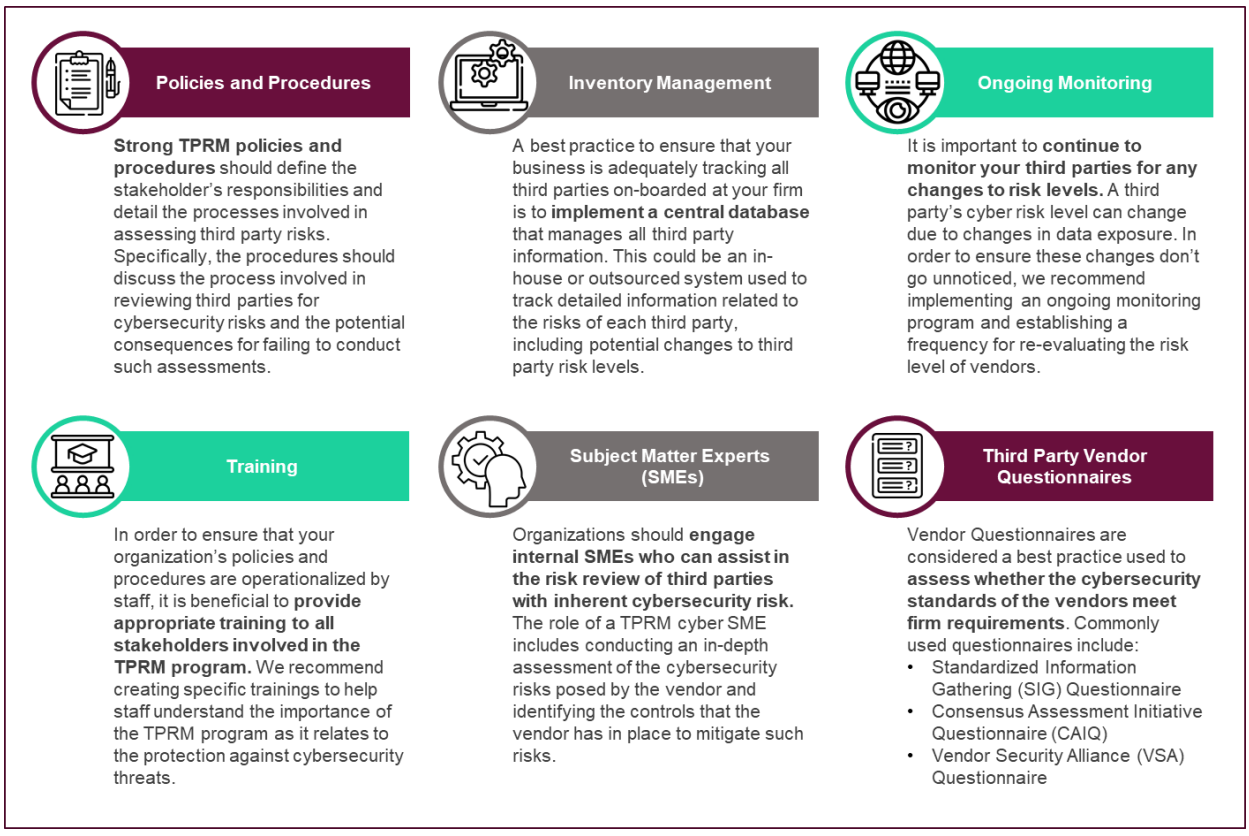
[1] Source: Matthew Schwartz - BankInfoSecurity

[2] Source: OCC Spring 2020 Semiannual Risk Perspective

Operational Risk	Causes	Best Practices / Control Considerations
Growing Cybersecurity Vulnerabilities Related to the Implementation of Teleworking Strategies	Utilization of teleworking strategies using VPN, virtual conferencing services and various additional remote telecommunication tools	Configure, secure, and monitor new teleworking tools as appropriate - Segment and secure bank networks as necessary if employees are connecting to bank systems via personal devices
Strained Telecommunications Capacity	A rise in usage of online and mobile bank systems by employees, customers, and third-party vendors	Properly manage technology infrastructures to allow for expanded telecommunications bandwidth when necessary to support and sustain suitable service levels
Increased Risk of Fraud and Possible Exposure of Confidential Customer Information	Sensitive processes that are executed beyond bank sanctioned properties and/or not using authorized bank technology	Perform relevant monitoring and surveillance such as utilizing data loss prevention technology, callback procedures, and increase cognizance of privacy and phishing mitigation procedures among bank staff
Growing Challenges to Existing Change Management Processes	Swift all-encompassing implementation of new bank systems which includes automation or business processes aimed to tackle developing operating environments and demands of customers	Strong third party risk management practices administered based on level of risk and change management as appropriate
Curtailment in Service Delivery Levels	Organizational responses to the COVID-19 pandemic and other related operational problems	Thoroughly examine operational workloads and third party vendor performance to address potential reductions in service levels punctually while simultaneously continuing to meet customer needs

TPRM Cybersecurity Best Practices

In addition to the OCC's guidance outlined above, there are standard key best practices that organizations should consider in order to mitigate cybersecurity risks specifically related to TPRM programs. The following best practices are focused on ensuring your business has a strong TPRM program in place that addresses and protects against cybersecurity risk.



Third Party Vendor Questionnaires

The table below outlines the vendor questionnaires mentioned above in further detail. Each questionnaire has a different approach and focus. These assessments should be leveraged depending on a vendor's function within the organization and its inherent cybersecurity risks.

Common Third Party Questionnaires to help assess Cybersecurity Risk	
Standardized Information Gathering (SIG) Questionnaire	• The SIG is a popular questionnaire containing over 1,000 questions. The questionnaire can be customized based on the vendor and its inherent risks. • The SIG 2020 version contains new cybersecurity requirements including, but not limited to, New York Department of Financial Services requirements, call center controls, sanctions compliance, Anti-modern slavery and human traffic regulatory controls, and Privacy regulation (CCPA).
Cloud Security Alliance - Consensus Assessment Initiative Questionnaire(CAIQ)	• The CAIQ documents security controls that exist in IaaS, PaaS, and SaaS. • The questionnaire helps businesses understand a third party's compliance with the Cloud Control Matrix (CMM).
Vendor Security Alliance (VSA) Questionnaire	• The VSA questionnaire was created by a coalition of companies to help streamline and standardize security assessments. • The VSA has two free questionnaires that corporations can leverage, which are updated annually. • The VSA – Full focuses deeply on vendor security, which the VSA – Core consists of a privacy section, as well as the most critical vendor security questions.

Advantages of Strong TPRM Cybersecurity Practices

Going beyond the minimum regulatory requirements and implementing a robust TPRM program enables businesses to acquire an in-depth understanding of their third party relationships, including the level of cybersecurity risk posed by each relationship.

Strong TPRM cybersecurity practices require businesses to work with each third party during the onboarding process to ensure that cybersecurity risk is controlled at a level that is accepted by the business's internal cybersecurity team. Furthermore, strong practices ensure that third parties are continually assessed for evolving risks.

In summary, with the right personnel and program in place, businesses will have a better understanding of which third parties have access to their data and how that data is used. This can reduce the likelihood of a cybersecurity breach caused by a third party occurring within an organization. In the case where a breach does still occur, strong TPRM cybersecurity practices will, at minimum, ensure a company is well prepared to react.

Key Questions for Management to Consider

Implementing effective third party cybersecurity measures can be challenging because there are more devices and users than ever today, creating a wider surface area to be exploited by potential attackers. Furthermore, as a result of COVID-19, an ever-increasing number of people are working remotely with sensitive and/or confidential customer and firm data. As attackers are becoming more innovative due to the upsurge of people working from home, firms must ensure that their third party entities have vigorous controls in place with respect to their internal cybersecurity practices. Conducting due diligence prior to vendor onboarding and regular third party audits and risk assessments are critical. Below are a few key questions management teams should consider while evaluating the robustness of their third party cybersecurity risks and vendor assessment processes:

DATA PROTECTION AND PRIVACY

- How does your firm protect private and/or proprietary data?
- What are the overarching legal obligations your entity has in protecting your data and the privacy of customers?

GOVERNANCE

- How can your business ensure that its TPRM Program(s) and/or functions are reasonably governed, controlled and overseen?
- How are cybersecurity roles and responsibilities defined?

TRAINING & AWARENESS

- How can your firm increase cybersecurity training and awareness for stakeholders engaging in new agreements with third parties?
- Are policies and procedures related to TPRM cybersecurity shared and communicated with all relevant stakeholders?

How Can Sia Partners Help?

In consideration of these enhanced cybersecurity challenges posed by third party vendors and magnified by remote working and virtual communication, Sia Partners is ready to assist our clients with their operational resilience needs with innovative and comprehensive solutions.

Sia Partners Service Offering Portfolio for TPRM Cybersecurity

Policy Design & Procedures Definition 	• Assist Information Security stakeholders to write or enhance policies and procedures including performing gap analysis and updating cybersecurity concerns in the master BCP. • Define and implement best practices in responding to cybersecurity incidents. Define an incident response plan to help IT staff detect, respond to, and recover from network security incidents and address issues like cybercrime, data loss, and service outages. • Facilitate change management process to implement enhanced procedures.
Data Protection & Cloud Security 	• Support our clients in implementing protective digital privacy measures (such as Data Encryption, Data Loss Prevention & Data Privacy measures) and Cloud Security controls (using trusted software, managing asset lifecycles, considering portability of continuous monitoring). • Design and implement a database to track third party services used by an organization, ensure integrity among the data set and provide visualized reporting and dashboard solutions.
Third Party Risk Reviews 	• Perform evaluation of the cybersecurity risks associated with the services provided by the third party. • Sia Partners recognizes that cybersecurity risks posed by third parties are not static and require ongoing evaluation. Our SMEs can assist in ongoing evaluation of third parties to ensure they are meeting contractual and regulatory requirements and assure that risks are appropriately managed.
Vulnerability Testing & Application Security 	• Help define, scope and guide our clients' red teams and external penetration testers in order to identify cybersecurity vulnerabilities and deficiencies to be patched or repaired. • Implement security measures for websites, web applications and web services as well as at the application level that aim to prevent data or code within the application from being stolen. • Deploy local IT trainings and raise employees' awareness with regards to Phishing, Spoofing, and Social Engineering.
Governance, Risk & Regulatory Compliance 	• Support the development, design and enhancement of our client's cybersecurity programs including defining roles and responsibilities, policy and procedural support, and compliance with regulations such as State and Data Privacy regulations in combination with industry best practices. • Provide project management solutions to help the firm implement a robust Third Party Risk Management program.

YOUR CONTACTS

ERIC BLACKMAN
Partner
917-769-6278
Eric.blackman@sia-partners.com

LIANA MARZANO
Senior Consultant
732-403-4167
Liana.marzano@sia-partners.com

MAX GATES
Consultant
716-574-1085
Max.gates@sia-partners.com

RISHIN SHAH
Consultant
516-423-0166
Rishin.shah@sia-partners.com

ABOUT SIA PARTNERS

Sia Partners is a next generation consulting firm focused on delivering superior value and tangible results to its clients as they navigate the digital revolution. With over 1,400 consultants in 16 countries, we will generate an annual turnover of USD 280 million for the current fiscal year. Our global footprint and our expertise in more than 30 sectors and services allow us to enhance our clients' businesses worldwide. We guide their projects and initiatives in strategy, business transformation, IT & digital strategy, and Data Science. As the pioneer of Consulting 4.0, we develop consulting bots and integrate AI in our solutions.

Abu Dhabi | Amsterdam | Baltimore l Brussels | Casablanca | Charlotte | Chicago l Denver | Doha | Dubai | Frankfurt | Hamburg | Hong Kong | Houston | London | Luxembourg | Lyon | Milan | Montréal | New York l Paris l Riyadh | Rome | Seattle | Singapore | Tokyo | Toronto |

For more information, visit www.sia-partners.com

Follow us on **LinkedIn** and **Twitter @SiaPartners**