A TPRM Perspective – Cybersecurity Risk

Ben Sady, Tim Kahrs, & Desmond Lites

Cybersecurity risk is a critical component of an effective third-party risk management (TPRM) program, which typically sits under a cross section of leadership including operational risk and cyber risk. Understanding and managing these types of risk has been a growing focus for organizations in recent years, especially as they aim to enhance their TPRM programs. In 2021, the FBI's Internet Crime Complaint Center (IC3) received a record number of complaints from the American public: 847,376 reported complaints, marking a 7% increase from 2020, with potential losses exceeding $6.9 billion. Among the complaints received, ransomware, business e-mail compromise schemes, and the criminal use of cryptocurrency were among the top incidents reported.[1]

In today's connected environment, organizations are working with an increasing number of third parties. As a result, organizations have had to posture for a cyberthreat environment that continues to grow each year. Not only are organizations exposed to direct cybersecurity threats, but they must consider vulnerabilities and risks within their third parties and their potential impact.

Cybersecurity Risk

Cybersecurity risks relate to the loss of confidentiality, integrity, or availability of data/systems and reflect the potential adverse impacts to organizational operations (such as mission, functions, image, or reputation) and assets, individuals, other organizations, and the nation.[2]

Today, data is shared more frequently and at higher volumes with partners and suppliers, leading to increased data breaches and security incidents. Cyber actors continue to exploit known software vulnerabilities and weak authentication against broad target sets. As a result, attacks targeting organizations, their service providers, and other subcontractors, *i.e.*, Nth parties, remain an issue for organizations. Given the heightened threat environment, organizations must have a greater focus on protecting electronic data from compromise.

Many regulators remain firm in their stance that, despite using external service providers, organizations should maintain the responsibility of validating that outsourced activities are conducted in a safe and sound manner. While your organization may not be able to totally eliminate all threats, necessary steps can be taken to build safeguards to help identify and mitigate current and emerging risks that third parties pose to the organization. To successfully mitigate cyber risks, your organization needs to involve stakeholders throughout the enterprise, including your third parties, to check that the risk management framework and control environment are appropriate for the organization's size, structure, and complexity of operations. In addition, a thorough understanding of current and emerging risks and a well-developed control environment are essential to help decision makers make informed decisions; appropriately identify, measure, monitor, and control risks; and prevent potential supervisory action and/or penalties.

Cyber Control Best Practices for Third Parties

Vendor contracts and independent assessments are two important focus areas for an organization as it assesses and manages third-party cyber risk. Maintaining effective cyber control is critical to the success of a cyber risk program. Cybersecurity control best practices and important expected controls are outlined below.

Examples of Expected Security Controls

In assessing the control environment of third parties, management can reference one of the recognized technology frameworks and industry standards, including the NIST Cybersecurity Framework, Control Objectives for Information and Related Technology (COBIT), and the International Organization for Standardization (ISO) 27000 series, among others.

Here are some example controls to help mitigate your organization's vendor cybersecurity risk:

- **Zero Trust**: Implement zero-trust security measures for your vendors and their vendors to help reduce implicit trust and require user and system authentication at multiple points in your IT stack
- **Data Security**: Require security controls be implemented at your vendors to help protect sensitive data at rest, in use, and in motion
- **Cloud Security**: Extra attention during control environment evaluation should be given to critical cloud service providers due to limited regulation for these types of vendors and growing reliance on cloud services
- **TPRM Platforms**: Check that vendors and their vendors are using the latest integrated solutions to assess and monitor risk in real time
- **BCP & DRP**: Verify that vendors have business continuity and disaster recovery plans in place to decrease the downtime and cost of an incident, as well as improve response time
- **Backups**: Organizations should make sure vendors and their vendors have effectively implemented and regularly tested backups for key systems to provide operational resilience, including maintaining a backup of critical data in the event malware encrypts or corrupts systems
- **Threat & Vulnerability Management**: Vendors should provide evidence they have developed heightened threat and vulnerability monitoring processes and implemented more streamlined patch management processes
- **IAM**: Certify that vendors are using enhanced identity and access management solutions, including solutions such as multifactor authentication and privileged access management
- **System Configurations/Hardening**: Organizations should check that vendors and their vendors improve the hardening of system configurations and timely change/patch management
- **Nth Parties**: Verify due diligence and data protection controls are in place for subcontractors of your third parties

Contractual Requirements

If the third-party service provider stores, transmits, processes, or disposes of customer information, management should require third-party service provider to make best efforts to implement appropriate measures designed to meet established security standards. Organizations can help facilitate this assurance by requiring that the following cybersecurity risk components are incorporated within the vendor contract:

- Minimum control and reporting standards
- Clearly defined roles and responsibilities across the cybersecurity risk program
- Specify that the institution or an independent auditor has access to the service provider to evaluate the service provider's performance against security standards

Furthermore, as a continuous monitoring best practice, processes should be established to periodically review existing contracts to continually address pertinent risk controls and legal protections.

Independent Assessments

As part of the oversight of third-party service providers, management should evaluate whether cyber risks are required to be assessed and reported on to their customers. Management may use the System and Organization Controls (SOC) report to complement the organization's internal activities and use an independent assessor to verify that the third-party organization is following industry best practices.

The dedicated national SOC & HITRUST team provides SOC readiness assessments and SOC 1 Type 1, SOC 1 Type 2, SOC 2 Type 1, SOC 2 Type 2, and SOC 3 examinations to help organizations assess and report on the design and operating effectiveness of their internal controls. Please refer to our SOC & HITRUST Solutions page for more information on our offerings.

Why Now & How Can FORVIS Help?

Companies have increasingly relied upon third-party products and services to help drive strategic and operational efficiencies within the organization. Growing pressures from the competitive marketplace aren't expected to change this trend in the coming years. Organizational stakeholders should understand all the risks associated with any third-party relationship to evaluate the opportunity effectively. A thorough understanding of current and emerging risks and a well-developed control environment are essential and help prevent potential supervisory action and/or penalties. Transparency around potential cybersecurity risk exposure is especially important as it's a growing focus area of third-party relationships. Not only are organizations exposed to direct cybersecurity threats, but they must consider vulnerabilities and risks within their third parties and their potential impact. In an ever-changing landscape, navigating this can be challenging and time-consuming. **FORVIS** can help your organization design a strong third-party risk management program and offers skilled resources to help operationalize effective TPRM processes.

If you have questions or need assistance, please reach out to a professional at FORVIS.

[1] *"Federal Bureau of Investigation Internet Crime Report 2021," ic3.gov*

[2] *"Integrating Cybersecurity and Enterprise Risk Management (ERM)," nvlpubs.nist.gov, October 2020*

Want more insights specific to Cybersecurity?

Scan the QR code to sign up for **FOR**sights™