cyber GRX

Mitigate Third-Party Cyber Risk Exposure

Top Three Ways to Kickstart Your Third-Party Cyber Risk Management Program

Table of Contents

Introduction

Outsourcing, digitization, and globalization - the three main drivers of business transformation over the last 30 years. From these forces, organizations have prospered from the innovation of new products and services, the ability to focus on their core competencies, reduced costs and new global markets.

But with agility comes cyber risk.

Globally dispersed, highly networked and digitized businesses now face new cybersecurity and resiliency risks that many businesses are just now beginning to address. As a result, both government and commercial enterprises are establishing third-party cyber risk management (TPCRM) programs to better identify, assess, mitigate and oversee the risks created by third-parties, partners, and customers in their digital ecosystem.

Previously, time-consuming and often costly regulatory requirements mandating TPCRM programs only affected organizations working in highly regulated industries, such as financial services, healthcare and energy. But today, all organizations require a scalable and cost efficient TPCRM program to protect their company and to drive regulatory compliance.

Evolution of Third-Party Cyber Risk Management

TPCRM today is complex, inefficient and expensive; more slanted toward compliance than risk mitigation. There are three major factors that reinforce the need to apply a new approach to TPCRM, and start shifting from static and compliance-based approaches to dynamic and scalable approaches:

1. Expanded use of third parties and cloud providers in the enterprise:

    a. According to Deloitte's 2018 Global Outsourcing Survey, companies are broadening their approach to outsourcing as they view it as more than a simple cost-cutting play. Outsourcing can enable competitive advantages and access to modern and disruptive technologies, like cloud providers and even robotic process automation (RPA).

    b. Organizations looking to work with third parties must balance the flexibility and convenience with the need to reduce vendor risk. In many cases, significant amounts of information exchange and network access are involved in these business processes, which dramatically increases risk—and the one thing that cannot be outsourced is vendor risk management. Organizations lack oversight, as 75% of Aravo's 2018 Third-Party Risk Management survey respondents state they do not have a complete inventory of all third parties that handle personal data related to employees and customers.

2. Rise in the number of attacks that originate from a third party:

    a. Fortune 500 companies typically have between 10,000 and 80,000 third parties. It only takes one, like a mechanical contractor, to be compromised and allow the attackers to ride in on a trusted connection. According to Soha Systems, over 63% of all breaches stem from third-party vendors. According to TechNews-World, around 80% of data breaches originate in the supply chain. Attackers are lazy and opportunistic and take the path of least resistance to getting their hands on your data.

3. Increased Regulatory Scrutiny

    a. 2018 has been a banner year for big cybersecurity regulations, with the implementation of the General Data Protection Regulation (GDPR) in May, the Asia Pacific Data Protection and Cybersecurity Regulation in full effect, and many other nations and regions following suit.

b. In the US, more than 265 bills and resolutions related to cybersecurity have been introduced and considered this year, according to NCSL.org. The California Consumer Privacy Act (CCPA) has been trailblazing the way for many states, with a January 1st, 2020 deadline that enacts broad privacy requirements that keep businesses accountable for the personal information they collect. On the East Coast, New York passed the NYDFS Cybersecurity Regulation, a new set of rules from the NY Department of Financial Services (NYDFS) that impose strict cybersecurity rules on covered organizations, from infrastructure defenses to documented disaster recovery planning. Currently, 22 other states have enacted 52 bills as well, and the trend is expected to continue gaining momentum (Cybersecurity Legislation 2018, NCSL.org).

c. Whether the regulation is state-imposed, country-imposed, or region-wide, there are strict, serious ramifications for failing to adhere to requirements. For example, GDPR fines can amass up to €20 million or 4% of world-wide yearly revenue – whichever is higher. This hefty fine applies to all companies throughout the world that touch any piece of an EU citizen's data, not just those located within the EU. Even state-centric regulations like the CCPA can cost an organization $7,500 per violation, which can cumulate very quickly for large and systemic abuses. The potential for such substantial fines is changing the way organizations approach their data protection practices.

Is your current approach truly protecting your sensitive data and assets? The majority of TPCRM programs are geared toward compliance and are not risk-based approaches. This compliance slant prevents organizations from truly working to identify and mitigate real issues based on actual threats and countermeasures. Not being compliant can cost you, but with **the average breach cost looming near $7,350,000 in the US,** it's time to take a dynamic approach to TPCRM and cover all of your bases.

Third-Party Cyber Risk – A Growing Challenge Backed by Facts

- According to Bomgar, an average of 181 vendors are granted access to a company's network in a given week.
- In the January 2017 report, SurfWatch Labs found "threat data collected and evaluated by SurfWatch Labs shows that the percentage of cybercrime linked to third parties nearly doubled over the past year – and that only includes publicly disclosed breaches."
- According to a Bomgar survey, 81% of respondents said they've seen an increase in third-party vendors over the last two years, and 67% have already experienced a data breach that was either definitely (35%) or possibly (34%) linked to a third-party vendor.
- Together, third parties deliver the majority of a company's revenue – 60% or more, according to Opus Research.
- A 2017 Ponemon Institute survey found that the cost of breaches is rising, with US companies paying an average $7,350,000 in breach fines, remediation costs, and loss of customers – a rise of 10% since 2016.

Top Three Ways to Kickstart Your Third-Party Cyber Risk Management Program

To fully grasp building a scalable TPCRM program, organizations must understand the three basic components of TPCRM:

1. Identify

2. Assess

3. Mitigate

1) **Identify** — Gain full visibility into your third-party ecosystem, including how you interact with each (i.e., Do they handle your data? Do they touch your networks?) and the potential risk that they pose to your organization. Understand the business exposure each third party imposes.

a. Work with procurement and supplier management to gain complete visibility into your current and future third parties.

b. Ensure audit rights are built into new contracts with third parties.

c. Build a mechanism to incorporate changes in your relationship (i.e., you utilize more/less of their services) and changes to their business (i.e., breach, divestiture, acquisition).

END STATE: A dashboard with all of your third parties tiered and risk ranked from high to low.

Caution: If you're not closely aligned with procurement, relationship managers and other stakeholders, your program will always be behind. Work diligently to convince your company that you should be involved in the front end of the relationship (read: RFP stage) rather than after the fact.

2) **Assess** — Perform an appropriate assessment on each tier to understand business exposure from each. Do not use spreadsheet-based assessments! Automate this process with technology that is scalable and secure.

a. High Risk - Perform a fully validated assessment (i.e., on-site) to ensure controls are in place for the asset classes touched.

b. Medium Risk - Perform a long-form self-questionnaire with a quality control discussion that requires the third party to discuss any questionable areas.

c. Low Risk - Perform a short-form self-questionnaire.

END STATE: A centralized dashboard that provides visibility into your entire ecosystem of third parties and status of their assessment.

Caution: If you store completed assessments in a GRC tool or other repository, but do not dynamically monitor the changing state of your third parties, your program will not have the ability to perform the appropriate level of due diligence.

3) **Mitigate** — Collaborate with each third party to prioritize remediation steps, track progress and drive to completion.

a. Collaborative discussions with each third parties to identify remediation steps

b. Associate timelines with each remediation step

c. Track progress

d. Drive remediation to completion with supporting evidence

e. Audit trail

END STATE: The ability to collaborate with third parties (with an audit trail) and automate and track the remediation progress of key findings.

Caution: Without the ability to automate communication steps via a platform (rather than email, phone or "shared spreadsheets"), your ability to scale your Third-Party Cyber Risk Program past 8-12 third parties will be limited.

Bonus Process to Streamline Your TPCRM Program

Continuous Monitoring — Schedule quarterly updates with your third parties that have had a state change (i.e., breach, acquired a company, etc.). Host calls with third parties to understand controls evidence from previous quarters' remediation strategies. Utilize dynamic data and other methods to understand security posture changes from your third-party ecosystem.

a. Ensure your third parties do not have a change in state due to a misconfiguration, introduction of new technology or applications, acquisition of a company that increases their digital footprint or suffers a breach.

b. Build mass collaboration capabilities in the case a vulnerability like Heartbleed is released.

END STATE: The ability to automatically correlate threat intelligence to weak controls in your digital ecosystem and place your focus on the third parties that pose the most threat to your enterprise.

Caution: Outside/In monitors can be helpful to understand security posture changes that are visible from the outside. But, they provide no visibility into internal issues. Only when combined with an internal assessment is an Outside/In scan deemed reliable.

It's Time to Wipe the Slate Clean and Take a New Approach to TPCRM

Third-party cyber risk management is a critical component to any organization's security, but many third-party programs are plagued with outdated and inefficient processes that drain resources and provide little insight. As third-party related breaches continue to increase, it's time to apply a modern approach to TPCRM.

CyberGRX has transformed the way the market conducts third-party cyber risk management by replacing static and siloed methods with a dynamic and collaborative approach that unites third parties and their customers in the fight against cyber threats. While organizations and third parties face different challenges in third-party risk management, CyberGRX has proven that organizations are stronger when they work together. The CyberGRX Exchange breaks down barriers between third parties and their customers, enabling them to share dynamic data and create actionable insights on how to prioritize and reduce their collective risk.

Conclusions

- You'll need buy-in from other stakeholders to scale and streamline a successful TPCRM program.
- Design a program that includes people, process and technology that optimizes and automates each stage of the process.
- One of the most important components of a successful program is to have a dashboard that provides visibility into your all of your third parties (tiered according to risk) and their changing nature.
- Performing a risk assessment and then storing the data in a GRC tool may assist your compliance efforts, but provides little value to reducing risk.
- Design a program that helps you focus your energy on the third parties that, if breached, will do the most damage to your business.

Where are you in your TPCRM journey? Take our maturity quiz to gain insights on next steps, or contact us to learn more about how CyberGRX can force multiply your third-party risk management program.

Ready for a free trial? **cybergrx.com**

MassMutual FINANCIAL GROUP · Rally Ventures · TENELEVEN · PINNACOL ASSURANCE · TRUSTED AND RECOMMENDED BY · Blackstone · ADP · aetna · ALLEGIS CAPITAL · BESSEMER VENTURE PARTNERS