cyberGRX

Mitigate Third-Party Risk Exposure

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

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 cyber security and resiliency risks that many businesses are just now beginning to address. As a result, both government and commercial enterprises are establishing third-party 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.

Time-consuming and often costly regulatory requirements mandating TPCRM programs previously 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 Risk Management

TPCRM has evolved to be complex and expensive; more slanted toward compliance than risk mitigation. There are three major factors driving the need to enhance and scale TPCRM programs today:

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

- According to Deloitte's 2016 Global Outsourcing Survey, companies are broadening their approach to outsourcing as they begin to view it as more than a simple cost-cutting play. Organizations are increasingly outsourcing key processes to third parties and using an ever-wider range of vendors in their supply chains.

- 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 74 percent of 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:

- 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 PWC's The

Global State of Information Security Survey 2016, over 50% of all breaches come from third-party vendors. Accord ing to TechNewsWorld, around 80 percent of data breaches originate in the supply chain. Attackers are lazy and opportunistic and take the least path of resistance to getting their hands on your data.

3. Compliance vs. risk management:

- 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.

4. Costs:

- When TPCRM became part of most security and risk organization's strategy, budget was easy to come by. Leaders said, "Fix the problem at all costs." Today, business leaders are looking for ways to address the growing third party risk problem while simultaneously driving economic efficiency.

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

- According to PwC's 2016 Global State of Information Security report, third-party contractors are the biggest source of security incidents outside of a company's employees.
- 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."
- In a June of 2016 Ponemon Institute survey, 55% of small- and medium-sized businesses experienced a cyber-attack in the last 12 months, with 41% saying they were impacted by third-party mistakes.
- Approximately 66% of companies extensively or significantly rely on third-party third-parties. According to The Institute of Internet Auditors Research Foundation (IIARF) survey, another 34% moderately used third parties. Collectively, just 1% of respondents used very few third-parties.
- The average company's network is accessed by 89 different third-parties each week.

Top Three Way 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 your inherent risk from each third party.**

   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 residual risk 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
   d) No Risk - Monitor these third parties for state changes that require due diligence

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 & 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 quarter's remediation strategies. Utilize 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.
a) 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.

A Proposed Design for a New Era of TPCRM

To mitigate the complexity, risk and costs of TPCRM, a platform model that benefits both third-parties and customers is needed. The key is providing technology that benefits both sides.

The industry requires an "S&P for risk assessments" model that connects third parties and customers. This exchange allows third parties to share updated risk assessment data with up-stream partners. It also allows customers instant access to fresh risk assessments to enable speed and accuracy.

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 and optimizes & 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 you 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.

If you need additional assistance, contact sales@cybergrx.com