Agility and Resiliency in your TPRM Program

November 18th, 2021

Your Speaker

Rick Merhai
Head of Third Party Risk
Program & Strategy

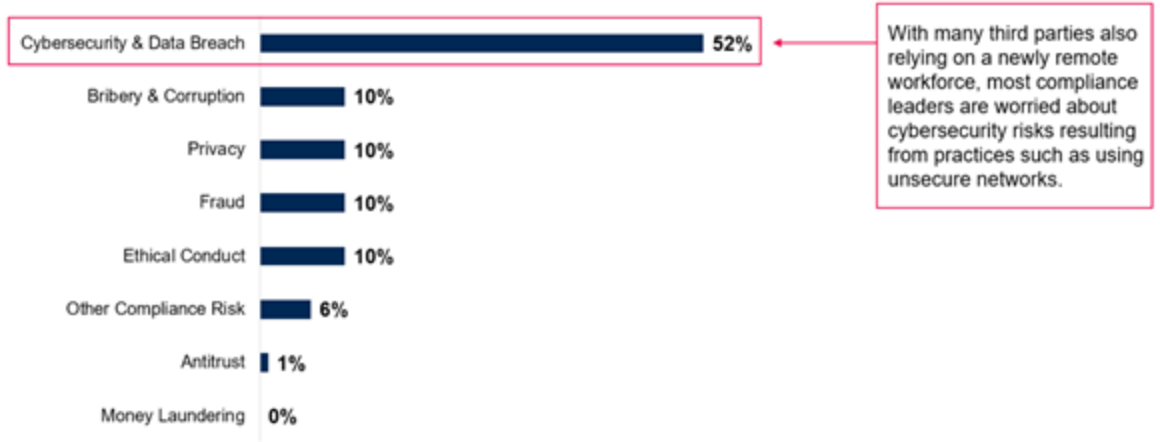
Cybersecurity is a Top Concern

37% of financial services CISOs have seen an increase in cyberattacks and **49% express greater concern about cyber attacks** due to WFH. (IDG)

Some **40% of organizations have experienced a data breach caused by a third-party**, while half have suffered an outage. (EY)

The impact of COVID-19 on supply chains and operations **has revealed gaps** and fragmentation in some organizations' approach to third-party risk management. (Deloitte)

Figure 1. Which third-party compliance risk has increased (or could increase) the most at your organization as a result of COVID-19?



n=145

Source: Gartner's COVID-19's Impact on Third-Party Risk Management Webinar Poll; 14 April 2020

Why is managing Third Party Risk Important?

Third party data breaches and cyberattacks account for over half of all data breaches. "As data breaches within corporations and governments continue to rise, the expenses to recover from them are escalating at an exponential pace.

"According to a study by the Ponemon Institute and IBM, the average cost of a data breach is $3.92million, up 6.4% (in 2019) compared to previous periods. With 3rd party breaches, there can be additional costs beyond the usual financial, regulatory and reputational damage that a data breach can bring. The availability and resiliency of services provided by our 3rd parties could be impacted.

The cost of data breach study showed that data breaches had a huge negative impact of customer trust, which led to lost of business. Lost business was the largest of the four major costs that contributed to the total cost of a data breach. The average cost of lost business was $1.42 million and caused 3.9 percent of customer churm.

"Data breach costs have a multi year impact - …"53 percent of breach costs are typically realized in the first year, 32 percent in the second year and 16 percent more than two years after the breach"

Every day, businesses experience cybersecurity incidents that can become disruptive, costly, and significantly damage their reputation.

Source: McKinsey, Covid-19: Briefing Materials, June 2020

4 Forces Shaping the New Normal

Metamorphosis of Demand

20-60% more consumers are now digital

An Altered Workforce

Remote workforce is the new norm

Regulatory Uncertainty

New regulations favoring local economies and privacy concerns

Recovering from the Virus

New strains of the virus constantly

Source: McKinsey, Covid-19: Briefing Materials, June 2020

Challenges

Point in Time Assessments

Limited Due Diligence Capabilities

Manual and Inefficient Processes

Third-party risk management is evolving

Previous years have shown ‘chronic underinvestment’

Many organizations are now taking steps to get-ahead (competitive advantage)

However, TPRM remains in its infancy

Companies are looking to mature their TPRM this year with cutting-edge technology and more robust operating models

"Organizations are more worried about regulatory scrutiny than last year: 49% cite it, up from 43%." *Deloitte*

Key considerations when enhancing your third-party risk management program

1. Think about cybersecurity earlier during the vendor onboarding process

2. Go beyond trust, but verify with the addition of validation and continuous monitoring

3. Make cybersecurity part of your contracting process

1 Cybersecurity from the start

When does your assessment process start?

- During the RFP process?
- After the contract has been signed ?
- When there's a third-party security threat or breach?

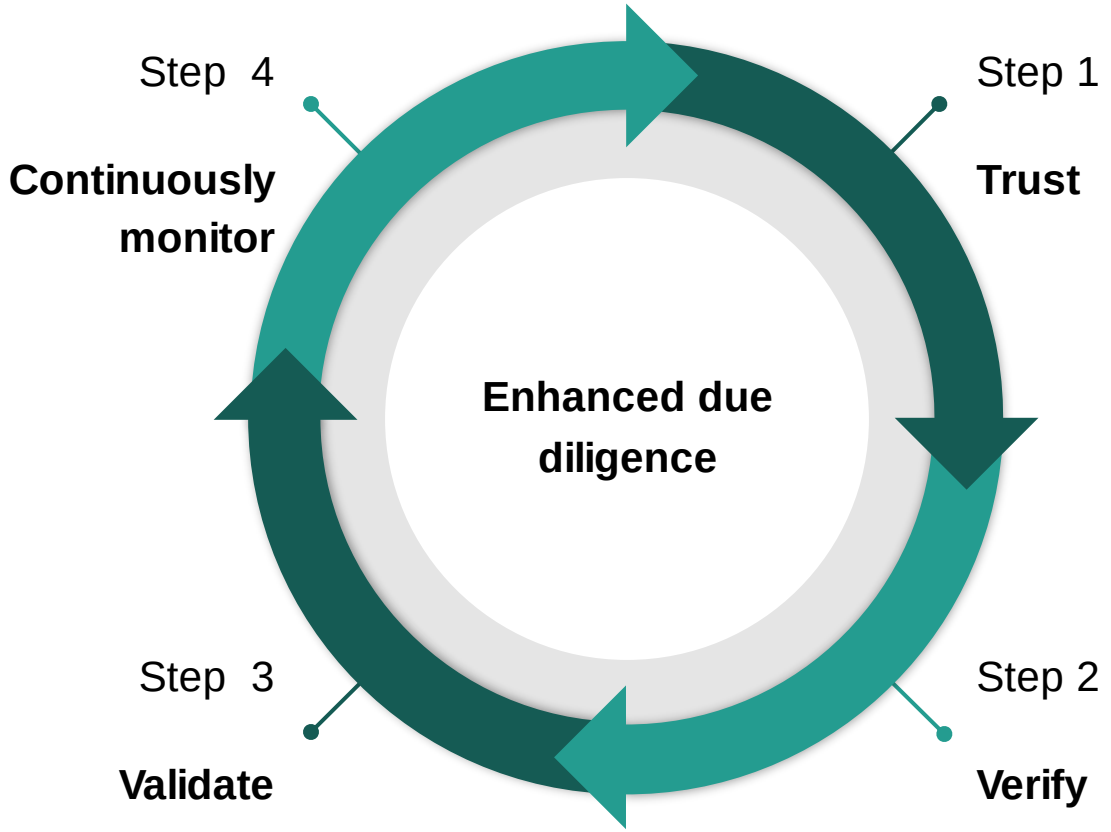
It's important to understand the cybersecurity posture of your vendors even before contract signing.

Vendors and third parties to any organization can provide a small, one-time need for a single project, or can be an ongoing business partner.

Understand the level of inherent risk of working with a particular third party. Utilize RFP questionnaires to understand if they meet your control requirements.

2 Trust, verify, validate, & continuously monitor

The OCC cites "continuous monitoring" as part of an effective vendor risk management framework for the finserv industry.



Trust by verify

It's important to set expectations with your third parties, however, verifying that they are taking steps to reduce risk is also a necessary part of the third-party risk management process.

Trust

- You trust that your vendors understood and answered the assessment accurately

Verify

- Develop a process and apply appropriate assessment tools and techniques
- Verify assessment responses via the collection of artifacts

Validation and continuous monitoring

Without validation and continuous monitoring, you leave your organization open to significant regulatory risk and reputational damage when things don't go as expected.

Validate

- Incorporate tools that help you validate with data

Continuous Monitoring

- Point-in-time assessments can find vulnerabilities at a single moment, but they fail to monitor activity between the assessments

3 Cybersecurity in the contracting process

Examples of what to include in contract language for third-party access to sensitive data:

- Ensure supplier meets organization requirements
- Define roles and responsibilities
- Data security contract language
- Special notes about applicable compliance regulations

Contracts play a part in managing risk exposure with your third parties

MSAs tend to get stale very quickly. It's important to ensure that updates are made as your organization evolves

"Right to audit" clauses give your organization peace of mind

Q&A