BRC
BOARD RISK COMMITTEE
BOARD RISK REPORT

April 20, 2021

WHAT BOARDS SHOULD KNOW ABOUT THIRD PARTY RISK

By Brenda Ferraro

Boards continue to be extremely focused on risk management issues as the headlines reflect the pandemic, a sharp increase in disruptive cyber-attacks, and emerging Environmental, Social, and Governance (ESG) issues worldwide. The pandemic has accelerated presidential executive orders with a focus on the management of extended enterprise and complex supply chains. All boards must gain a better understanding of how increasingly complex supply chains increase attack surfaces and make the companies they oversee more vulnerable. Every board should have confidence that third party risks are at least as well managed as those inside their organization's four walls, and that when significant disruptions do occur their organization can recover quickly.

BOARD OVERSIGHT – UNDERSTAND WHAT MATTERS MOST

Every board should have a good understanding of how Third Party Risk Management (TPRM) programs are structured and have a means to periodically judge the effectiveness of those programs. The pandemic has accelerated the awareness of the trend toward more complex supply chains and the need for companies to adapt their due diligence processes accordingly. Boards should feel confident that third party due diligence processes are based on relevance, well suited to the current environment, and can pivot quickly if required.

Understanding how companies are adapting to this challenge has become increasingly important. Many companies are expanding their use of virtual assessments to conduct the "validation" portions of examinations they previously conducted onsite. TPRM programs have increasingly turned to continuous monitoring techniques to evaluate the cyber hygiene, financial stability, and other key characteristics of companies to gain more timely insight into risks.

Questions the Board should consider include:

- Does my organization maintain a complete vendor inventory, distinguishing third parties that support critical functions? Does that inventory include known fourth (or Nth) parties supporting critical functions?
- Are third (and Nth) party relationships effectively mapped, showing interconnections and the function(s) of each vendor?
- Do our vendor assessments include our third party vendors and, wherever possible, our fourth, and Nth party vendors?
- Does our organization have an effective continuous monitoring program to monitor the cyber hygiene (and other aspects) of our vendors?
- Do we regularly test incident recovery procedures with vendors supporting important products or services?
- Does our organization have a single point of failure or a concentration risk where a single vendor is supporting multiple important services?
- Do we regularly perform an arm's length evaluation of our TPRM program's effectiveness?

THE BOARD'S ROLE IN INCIDENT MANAGEMENT OVERSIGHT

At a time when complex supply chains may increasingly lead to unexpected incidents, it's more important than ever that strong board oversight is extended to the incident management process. Significant

incidents may arise from downstream vendors in complex supply chains and – as a consequence – organizations may not quickly understand an incident's source. Also, complex supply chains may make it more difficult to assure acceptable restoration of services where the root cause of a problem may be difficult to rapidly identify.

Proactive third party programs reach out to vendors to help them resolve issues in the short term, while at the same time help suppliers enable better longer term security hygiene. Boards will want to encourage this type of proactive vendor outreach which will have a material impact on the issue resolution process.

Boards should consider the following questions:

- Has the board participated in tabletop or other exercises that simulate material incidents? When these incidents involve a third or Nth party, have these exercises simulated who will communicate with various stakeholders and when those communications should occur?
- Is the organization confident that it has tested recovery scenarios that include circumstances where a vendor may not be able to recover its operation within an acceptable time frame?
- Is the organization confident it can respond effectively to far more frequent ransomware attacks, whether in-house or at a vendor?
- Does the organization keep a record of incidents and their resolutions, incorporating learnings from those incidents into improved TPRM processes?

HOW COMPLIANCE AND REGULATORY CHANGES IMPACT BOARD OVERSIGHT

Boards should have a continuing sense of how the regulatory environment is changing and where those changes may affect the organizations they oversee. In situations where organizations operate internationally, monitoring and influencing the legislative agenda is a more complex process.

More and more regulatory initiatives are requiring organizations to utilize best practices to ensure compliance, a trend tied to the heightened threat landscape. Since September there have been at least seven new or updated resilience and/or third party regulations issued by major regulators around the world.

Boards should ask questions that include:

- Does our organization have an up-to-date understanding of applicable third party risk related regulatory expectations? Is our organization engaging with regulators to ensure it has good context around emerging requirements? How frequently is the board updated on changing regulatory expectations?
- When evolving regulations impose additional requirements on TPRM resources, does the board have the right information to authorize revised resources?
- Does our organization understand the direction of the regulatory environment in all the areas in which we operate, including in emerging areas such as ESG?
- Is our compliance program able to effectively incorporate rapidly changing expectations as the threat environment and regulatory expectations change?
- What are the potential fees or charges that are associated with compliance mandates?

ABOUT THE AUTHOR

Brenda Ferraro is a member of the senior management team at Prevalent and a US/UK Shared Assessments Steering Committee Member. She is a 2020 honoree of The Top 25 Women in Cybersecurity and The Most Influential Women in Arizona and recognized on the Tech Innovators list of the 2021 Leaders to Watch. Her strategic leadership has paved the way for organizations to recognize value, remove program complexities, perform compliance readiness, and implement a flexible enterprise risk solution.

WHO WE ARE

The Board Risk Committee (BRC) is a non-competitive thought leadership peer forum dedicated to Board Risk Committee members and Chief Risk Officers (CROs). The BRC is a trusted place for the exchange of ideas, best practices, and topics of interest. BRC is affiliated with The Santa Fe Group (SFG). SFG is a strategic advisory company providing unparalleled expertise to leading financial institutions, healthcare payers and providers, law firms, educational institutions, retailers, utilities, and other critical infrastructure organizations.

CONNECT WITH US