UNCERTAINTY, COMPLACENCY, OR CONFIDENCE—

PICK THE RIGHT PATH TO MANAGING THIRD-PARTY RISK

Organizations are investing in digital technologies to drive business into the future. This also means they're increasingly reliant on third-party vendors for outsourced services and solutions—expanding their attack surface and introducing more risk. While these relationships must be monitored, many businesses are still doing nothing—or have just started implementing assessments—which still leaves the door wide open for a security incident to occur.

THIRD-PARTY EXPOSURE IS NECESSARY BUT RISKY

70%
of organizations have a "moderate" to "high" dependency on external organizations, according to Deloitte research.

59%
of organizations have experienced a data breach caused by a vendor or a third party, according to Ponemon Institute.

90%
that suffer a software supply chain attack see a financial impact, according to CrowdStrike.

MANAGING THIRD-PARTY RISK IS NO EASY TASK, WITH MANY MAJOR CHALLENGES TO OVERCOME, INCLUDING:

No Comprehensive Inventory of Third-Party Relationships—
only 34%
of organizations have one [Source: Ponemon].

Lack of Resources—
only 37%
of organizations have sufficient resources to manage third-party relationships.

77%
of financial organizations report **five or fewer employees dedicated to vendor management**
[Source: Venminder, "State of TPRM 2019" report, December 2018].

THESE CHALLENGES PUT SOME ON THE PATH TO COMPLACENCY

54%
do not monitor the security and privacy practices of vendors, according to Ponemon data.

OR ON THE PATH TO UNCERTAINTY

Some businesses attempt third-party risk management (TPRM) with point-in-time assessments. But these are imprecise and won't provide the level of security your organization requires.

ONLY **15%**
of organizations have taken basic steps to protect against third-party threats.

ONLY **43%**
of organizations say their third-party data safeguards are sufficient to prevent a data breach.

LACK OF CONFIDENCE IN CURRENT APPROACHES

Types of Approaches

- Questionnaires
- Onsite assessments
- Penetration tests

Vendor Assessment Cadence

Monday—Do an assessment

Tuesday—Vulnerability appears

No visibility on impact or potential risk until next assessment

Current processes are valuable efforts to understand third party cyber risk but are not continuous, scalable, and staying ahead of this dynamic risk

CONFIDENCE IN CURRENT TPRM IS LOW

65%
of organizations rate their TPRM program as less than highly effective.

GET ON A PATH TO CONFIDENCE

When you are managing third-party risk, confidence comes from the ability to:

- **Immediately see and understand the cyber risk across your supply chain**
- **Target your resources to achieve significant, measurable cyber risk reduction**
- **Work with third parties to quickly and collectively reduce cyber risk**

BITSIGHT

Whether you are launching, growing or optimizing your third-party risk management approach, BitSight puts you on the path to having confidence—the confidence you need to make faster, more strategic cyber risk management decisions with the resources you have today.

For more information, please visit **www.bitsight.com**