BITSIGHT

Closing the Gap: Why Automation is Needed for Vendor Risk Management

SPEED

"IT USED TO TAKE WEEKS TO COMPLETE VENDOR ASSESSMENTS. NOW IT TAKES US HOURS."

MICHAEL CHRISTIAN, INFORMATION SECURITY MANAGER OF CYBER RISK AND COMPLIANCE, CABELA'S

A recent HSB survey found that nearly half of the data breaches in 2017 were caused by a third-party vendor or contractor. As organizations invest in creating or strengthening vendor risk management (VRM) programs, they must ensure they are leveraging technology-enabled automation to keep up with an ever-growing vendor base, as well as the speed at which cyber threats emerge. When automation is brought to vendor risk management, organizations gain three critical attributes that helps them get to risk reduction.

1) SPEED

According to a recent Navex Global study, the ability to promptly resolve newly identified risks is a top challenge for organizations' third party risk management programs. Traditional VRM assessments and communication methods often have long turnaround times, inhibiting the ability to obtain a quick and comprehensive view of an organization's security posture. This can create greater risk exposure for organizations or delay service provider value during the vetting process.

To make decisions in a timely manner, companies need to be able to access and aggregate data about their vendors quickly and efficiently. The speed at which organizations can comprehensively assess third parties is critical to the success of any vendor risk management program, and ultimately, the value delivered to the business.

How can organizations make risk-informed decisions quickly? More importantly, how can they trust the data on which those decisions are made with the utmost confidence?

When companies are able to make critical vendor risk management decisions rapidly, this speed enables them to drive business value and partner better with the business. Quicker vendor assessments and selection means less downtime. This allows them faster turnaround and more productivity when it comes to managing hundreds and sometimes thousands of vendors that affect their business' bottom line.

Security Ratings platforms like BitSight instantly show an organization's quantified security performance over time. When new threats and vulnerabilities emerge, organizations can instantly assess the impact on the third and fourth parties they monitor and follow up as needed.

SCALE

"BITSIGHT HAS ALLOWED US TO EXPAND OUR CURRENT SERVICE PROVIDER COVERAGE 6X WITHOUT ADDING ANY ADDITIONAL FTES."

JASPER OSSENTJUK, CISO, TRANSUNION

2) SCALABILITY

The number of vendors and other third parties in your ecosystem will continue to grow. This isn't going away — in fact, according to a recent report by Bomgar, on average, 181 vendors are granted to access a company's network in any single week, more than double the number from 2016. In fact, 81 percent of companies have seen an increase in third-party vendors in the last two years." The increasing popularity of the cloud, the introduction of new technologies, and increasing demands from the business ensure that your job is only growing in importance.

An increasing number of third and fourth parties are now connected to an enterprise. Most organizations are resource constrained and do not have enough people or time to adequately conduct due diligence on all of their third and fourth parties. This creates greater risk exposure and may increase the likelihood of a third party security breach.

Instead, organizations must leverage technology-enabled automation that allows them to streamline cybersecurity assessments and processes for their entire supply chain. Doing so means that organizations do not have to continually hire and throw more people at the problem, and they can instead focus their existing staff on reducing the most immediate risks.

How can organizations monitor an increasing number of vendors, suppliers, and third parties? More importantly, how can they monitor a larger vendor base with greater diligence and frequency?

BitSight enables customers to automate the continuous monitoring of third and fourth parties for their vendor risk management programs. Moreover, customers can monitor as many companies as needed on a continuous or frequent basis.

Specifically, BitSight can help organizations answer the following questions:

- On which companies should I focus my assessments or audits?
- Which questions should I put greater emphasis on in questionnaires, assessments, or other due diligence activities?
- When should I engage and request more information?

COLLABORATION

TO DATE, NEARLY HALF OF COMPANIES INVITED TO THE PLATFORM HAVE INCREASED THEIR RATING BY AN AVERAGE OF 37 POINTS.

ABOUT BITSIGHT TECHNOLOGIES

BitSight transforms how companies manage information security risk with objective, verifiable and actionable Security Ratings. Founded in 2011, the company built its Security Ratings Platform to continuously analyze vast amounts of external data on security issues. Seven of the largest 10 cyber insurers, over 90 Fortune 500 companies, and 3 of the top 5 investment banks rely on BitSight to manage cyber risks.

FOR MORE INFORMATION

BitSight Technologies
125 Cambridge Park Drive
Suite 204
Cambridge, MA 02140

www.bitsighttech.com
sales@bitsighttech.com

3) COLLABORATION

The most difficult aspect of vendor risk management isn't just identifying risk - it is working with vendors, suppliers, and third parties and giving them the resources they need to fix security issues. Getting to risk reduction quickly means that both organizations are communicating effectively, using data and evidence rather than conjecture to make progress.

Additionally, when working with vendors to fix security issues and strengthen security posture, it can be hard to prioritize what to fix first. For vendors with limited resources, understanding which actions will yield the greatest change and improvement is essential.

How can organizations have data-driven conversations with vendors? More importantly, how can both parties agree on what needs to be fixed first, and communicate progress to each other?

Organizations don't just benefit themselves when they help a third party remediate risks and improve security posture — these changes benefit the broader business ecosystem as shared third parties make security improvements.

In order to attain this level of collaboration, organizations need to access a common platform where they can review the same data and provide clarity around their security posture. The BitSight Security Rating platform provides organizations and their vendors with data and resources that are pivotal to these conversations.

CONCLUSION

With an ever increasing dependency on vendors and third parties, vendor risk management has become a big challenge for organizations worldwide. Technology-enabled automation is essential to solving this challenge. Automation enables repeatable processes, allowing humans to focus on the greatest risks. The BitSight Security Ratings platform is bringing automation to vendor risk management programs and delivering greater speed, scalability, and collaboration to this business process.

"TransUnion chose BitSight because we needed to scale our third party security management program and we knew we couldn't do it with more people, we had to be smarter."

TransUnion

- Jasper Ossentjuk, CISO, TransUnion

Watch the full video here: https://www.bitsighttech.com/resources/transunion-bitsight-video