The

BRAVE APPROACH

Automating Third-Party Security

Panorays

Part I

The Need for Third-Party Security

The online world is teeming with cyber threats. Not a week goes by without reports of massive data breaches, with some that remained undetected for months before being discovered. Clearly, cyber criminals are becoming more sophisticated in the way they gain access to personal and business data.

Often, they do so by targeting the weakest entry point: the third parties that are connected to the company. They can be connected through IT systems or integrations, and they can be SaaS vendors or third parties that hold sensitive data.

01

The

Facts About Third-Party Breaches

A data breach through a third party can wreak havoc on the organizations to which the third party is connected. Such breaches are increasing in severity and take place across all industries. Here are a few notable examples from 2018 alone:

- The notorious cyber criminal Magecart group succeeded in hacking major retailers, including Ticketmaster, Feedify, British Airways and Newegg, and exposing hundreds of thousands of records. In most of the attacks, the group hacked into a company that provided web application services through Javascript integration to other companies.

- The data of more than 2.65 million Atrium Health patients was breached through a billing vendor, AccuDoc Solutions.

- The personal data of at least 30,000 U.S. Department of Defense workers was exposed through a third-party vendor used for booking travel.

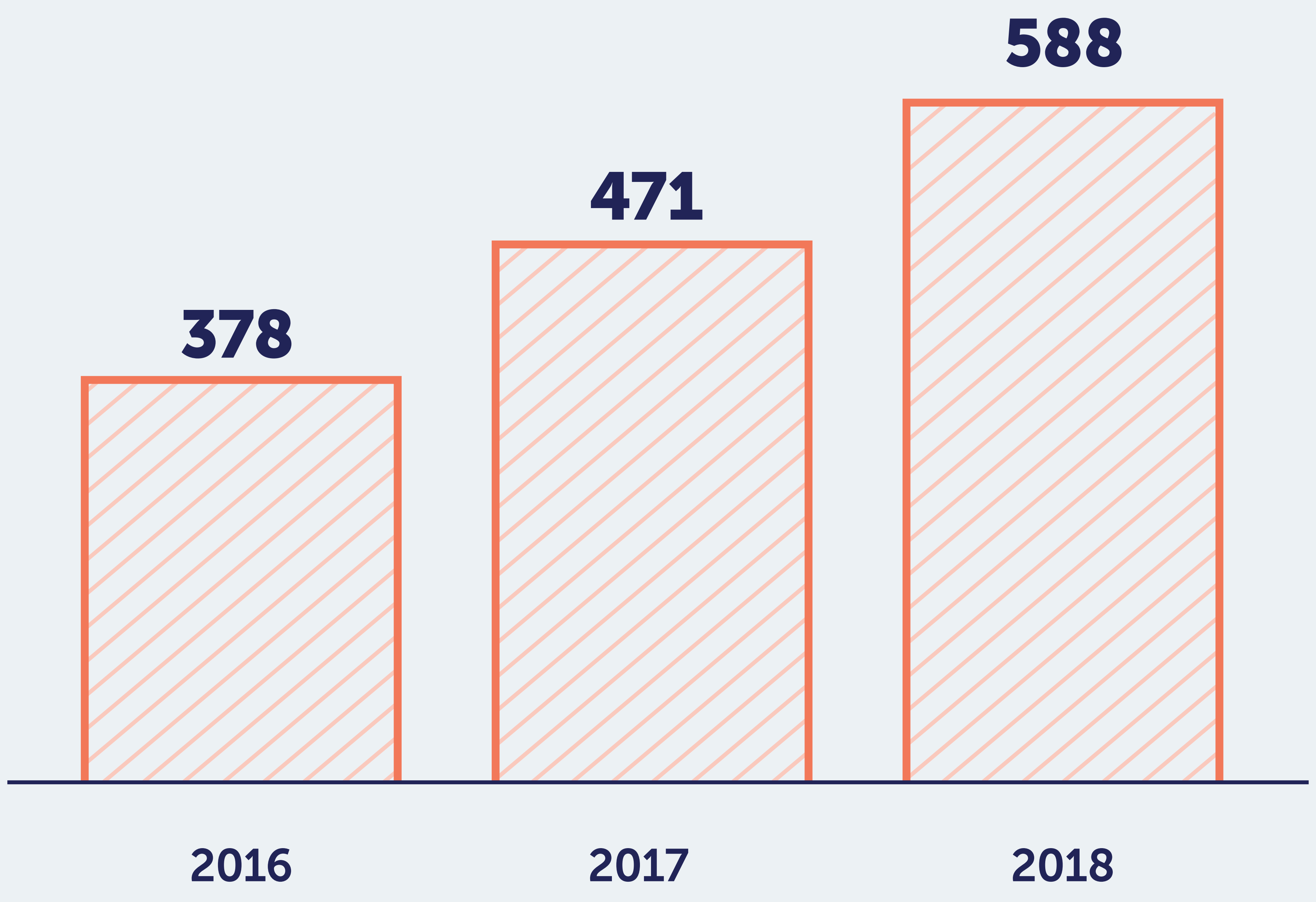
01

The

Facts About Third-Party Breaches

A recent study by the Ponemon Institute found that 61 percent of US respondents reported that their organizations experienced a data breach caused by one of their third parties. In 2017, this figure was 56 percent; in 2016, 49 percent. Moreover, the vast majority of respondents indicated that they had insufficient resources to manage third-party relationships.

Meanwhile, the number of third parties that companies are doing business with is increasing. The average number of third parties increased from 378 in 2016 to 588 in 2018.



Average Number of Third Parties

Source: "Data Risk in the Third-Party Ecosystem,"

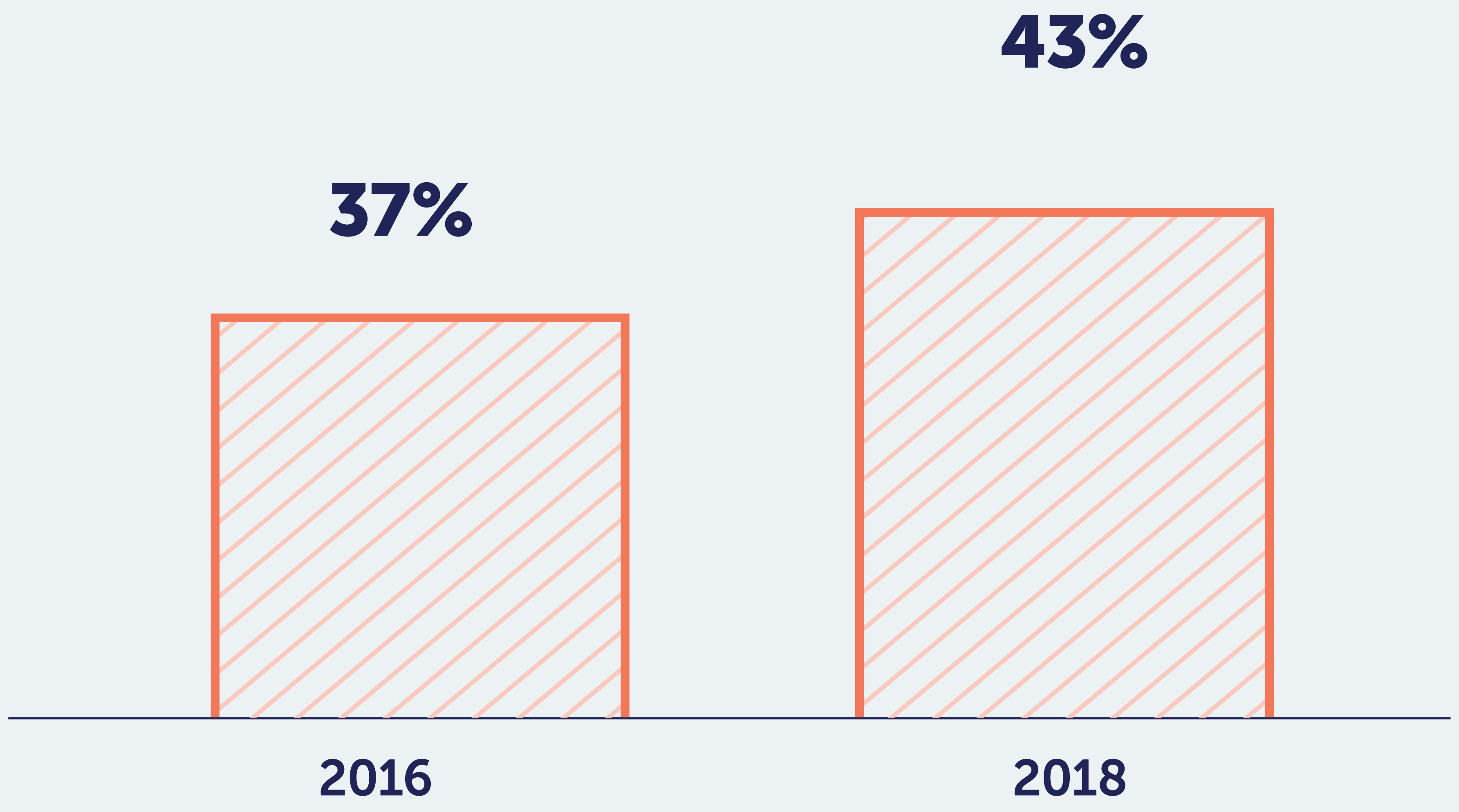
Ponemon Institute, November 2018

01

The

Facts About Third-Party Breaches

Along with these numbers is a rise in the percentage of third parties that share organizations' sensitive and confidential data, **from 37 percent in 2016 to 43 percent in 2018.**



Percentage Of Third Parties That Share Organizations' Sensitive Data

Source: "Data Risk in the Third-Party Ecosystem,"

Ponemon Institute, November 2018

01

The High Cost of Regulatory Penalties

Organizations have much more than just data to lose in a breach. Besides losing consumer confidence and loyalty, companies can face costly penalties for violating data privacy regulations.

Not complying with HIPAA can cost as much as $1.5 million per year for each violation category. The fines for not complying with the EU's General Data Privacy Regulation (GDPR) could be up to €20 million or 4 percent of annual revenue—whichever is greater. And the California Consumer Privacy Act—which is similar to GDPR and went into effect on January 1, 2020—fines $7,500 per violation.

To get a sense of what it might cost a business that does not comply with regulations, one need look no further than the recent $57 million GDPR penalty issued to Google. This was undoubtedly the first of many exorbitant fines that non-compliant businesses faced.

For all of these reasons, third-party security is a pressing concern for organizations. With increases in the number of third parties, sophisticated hacking techniques and data privacy laws, the problem is likely to only get worse.

01

Automation is Key for Third-Party Security Management

An important part of third-party security management involves audits in the form of questionnaires that must be completed by third parties for onboarding. Often, however, these audits are conducted using spreadsheets, resulting in an arduous, time-consuming and impractical process.

From a contractual perspective, organizations certainly have the right to audit their third parties, but fail to do so on a regular basis because of the cost, time and effort. Because of the complexity of cybersecurity management and the ongoing need to scale vendors, automating third-party security management is essential.

“The reality is that enterprises barely have the resources to check their own security,” says Amichai Shulman, cofounder and former CTO of Imperva. “Clearly, they are not in a position to be doing it for others.”

Part II

How to BRAVE the Third-Party Risk Landscape

Because of the high stakes involved, third-party risk and security is a daunting issue for many organizations. Ultimately, however, companies can be BRAVE about third-party security management by using automation. Organizations should use these five guidelines to achieve the best third-party security management:

- **B** Breadth
- **R** Rapid onboarding
- **A** Adherence
- **V** Visibility
- **E** Engagement

02

B

Breadth

As hackers become more sophisticated, the number of Web vulnerabilities continues to increase. According to a recent report by Imperva, the total number of vulnerabilities in Web applications jumped to 17,308 in 2018, climbing more than 23 percent compared to 2017—and that's just an example of WAF, which is only one attack vector.

Automation makes it possible to assess third parties in a comprehensive manner. As more vulnerabilities are discovered, they can be quickly added to an automated system which then monitors third parties for any trace of them, along with old threats as well.

Automation also makes it possible for companies to gain a continuous 360-degree view of third parties. Using advanced, cutting-edge knowledge about how hackers operate, automated security management can provide an outside-in view of third-party cyber gaps, while also managing security inquiries that consider an inside-out view of internal company policy and regulatory compliance.

02

R

Rapid onboarding

Many companies use spreadsheets to manage their third-party security. These manual processes, however, can be time-consuming. Matan Or-El, co-founder and CEO of Panorays, notes that companies without automation reported that it took an average of nine weeks to complete a security assessment. Because vulnerabilities keep being added, such spreadsheets are often outdated even before they are completed.

By contrast, automated third-party management can accomplish in hours what would take several weeks of manual processes. Such rapid processes ensure that companies can easily and quickly onboard their third parties. The ability to rapidly scale suppliers can help businesses grow without having to wait months for their third parties to be approved.

02

A

Adherence

Security assessments are not one-size-fits-all. A vendor that delivers office furniture, for example, probably will not have the same level of risk as a vendor with access to a company’s IT systems.

For this reason, evaluations should preferably be tailored to adhere to specific company policies and specifications in a manner that considers both the business relationship and the level of risk. Assessments should also provide a way to check that a supplier complies with specific regulations, such as GDPR, NYDFS, NIST or ISO.

This level of customization is difficult when using manual processes. Automated security assessments, however, can accomplish this rapidly and efficiently. Using automation, companies can choose a standard template or a template for a specific situation. If desired, companies can even create a completely new security assessment. Then they can easily determine which template is relevant to which supplier.

02

V

Visibility

Automation provides both companies and third parties with the ability to be continuously informed of:

- cyber threats and changes to cyber posture
- when third parties have received security inquiries and completion status
- questions to and from third parties
- third-party progress in mitigating cyber threats

With an automated third-party security solution, all parties involved in the process receive live alerts and can access more details with the click of a mouse. In addition, demonstrating security management and regulatory compliance to C-level executives demands comprehensive reporting. With automation, such professional reports can be generated promptly and easily for procurement, legal, compliance and security teams, as well as for board members and C-level execs. The right reports involve all teams, wherever they may be, spoken in the language specifically tailored to each team.

02

E

Engagement

Part of the challenge of managing third-party security is that doing so involves many different teams with completely different objectives. Vetting and hiring a third party begins with procurement, but it must involve the security team as well. At the same time, the legal department must be on board because it understands the requirements for organizational policy. Meanwhile, the third party—which is managed by a business person—must involve its security person to respond to a security assessment.

The process of hiring and managing third parties begins as a simple business transaction. Yet because of today’s cybersecurity and legal concerns, that transaction rapidly mushrooms into an overwhelming list of tasks that involves many team members.

Automation has the power to seamlessly and effectively involve all parties. Team members can easily engage and interact with each other on the same platform, no matter where they are located, and no matter what their roles are. Such engagement also removes friction by allowing companies and third parties to easily dispute findings and work together to close cyber gaps.

> "
>
> Automation has the power to seamlessly and effectively involve all parties.

03

Part III

Conclusion

More and more companies are adopting automation to cut down on paperwork, boost productivity, streamline processes and cut down on time. As this becomes the new standard for organizations, many business leaders are realizing that a failure to embrace automation ultimately leaves them behind.

With more companies depending on third parties than ever before, automation is particularly crucial to a comprehensive, effective and rapid third-party security management process.

Using Panorays' automated third-party management platform, companies and third parties can gain a competitive edge from all of the BRAVE features that automation offers. With Panorays' breadth, rapid onboarding, adherence, continuous visibility and engagement, companies and third parties can easily and securely work together.

About Panorays

Panorays automates third-party security lifecycle management. With the Panorays platform, companies dramatically speed up their third-party security evaluation process and gain continuous visibility while ensuring compliance to regulations such as GDPR, CCPA and NYDFS.

It is the only platform that enables companies to easily view, manage and engage on the security posture of their third parties, vendors, suppliers and business partners. Panorays is a SaaS-based platform, with no installation needed.

Panorays

Want to learn more about how Panorays can help your third-party security process?
Contact your Panorays sales rep or email us at info@panorays.com