Third-Party Risk to the Nth Degree

Managing the cyber risk of third-party vendors and their nth-party ecosystem

eSENTIRE

Table of Contents

INTRODUCTION

Third-party vendor ecosystems are not a new area of cyber risk, yet the subject still fails to be a top priority for many organizations. In an effort to understand why, in January 2019 eSentire and Spiceworks surveyed 600 IT and security decision-makers across a mix of industries and company size who have purchase influence over security solutions for their organization and a familiarity with third-party risk across a mix of company sizes and industries. Respondents were based in the U.S., Canada, U.K., Ireland and Scotland.

The intent was to capture current practices, to understand current business operations with third parties, types of data shared with vendors, and potential security practices/policies already in place. The survey aimed to quantify market concerns about third-party risk, determine top challenges, and identify potential areas of vulnerability. Subsequently, our goal is to ultimately provide quantitative and contextual measures by which your organization can compare current practices and investment to help mitigate third-party risk.

EXECUTIVE SUMMARY

Third-party risk, commonly known as vendor risk, is all about analyzing and controlling the fact that your data could be compromised by outside vendors and service providers. Companies increasingly use third parties to quickly scale and reduce costs. And, the use of new technologies such as IoT, mobile and cloud by vendors add to the question … where is my data and how can I protect it in someone else's hands? Many companies contract with third parties without considering data, operational and financial risks. And exposure at the third-party level can exponentially increase when considering 4th, 5th, and 6th parties (or nth parties) with whom vendors (and their vendors) do business. The more that companies outsource aspects of their business to third parties, the more complex becomes the web of risk.

This web makes it increasingly difficult to monitor third-party connections at the operational level, and more importantly, create policies that effectively minimize the associated risks. These research findings show there is an assumption of data protection by third parties that may not be valid and there is little consideration given to the data security of nth parties.

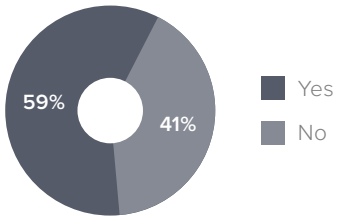
Survey results are backed by the initial assumption that companies fail to make third-party risk management a priority, and nth-party risk even less so. Respondents cited an absence of management support and a lack of resources and budget. Results also make it clear that there is misperception that correct practices are in place and that third parties are protecting respondents' data. In fact, 20 percent of respondents said they "trust" that their third parties will protect their data as a reason for not having a formal program in place, yet nearly half experienced a breach involving a third party in the past 12 months. And in only 15 percent of these instances was the breach discovered by the third party responsible.

Key Insight: Though most IT and security teams take a multi-step approach to evaluate third parties, formalized data policies and senior management support for third-party risk is lacking.

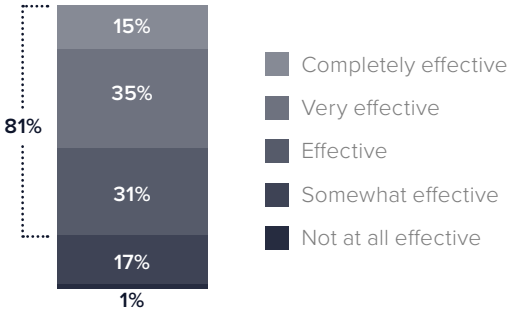
Approximately 60 percent of organizations surveyed have a formalized third-party data policy in place. The majority of those (81 percent) feel that their policy is effective, however only a small percentage (15 percent) believe that it is completely effective.

Only about a third of respondents (35 percent) completely agree that managing third-party risk is a priority at their organization, with several commenting that a lack of senior management prioritization and lack of resources and implementation knowledge is to blame.

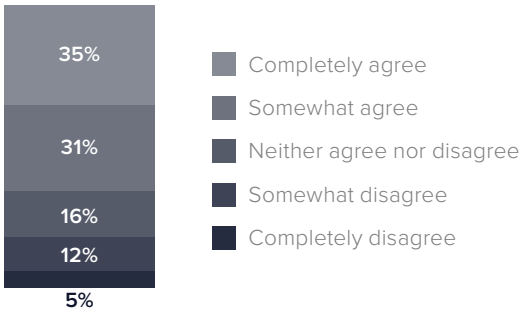
Third-party risk policy in place



Policy effectiveness rating



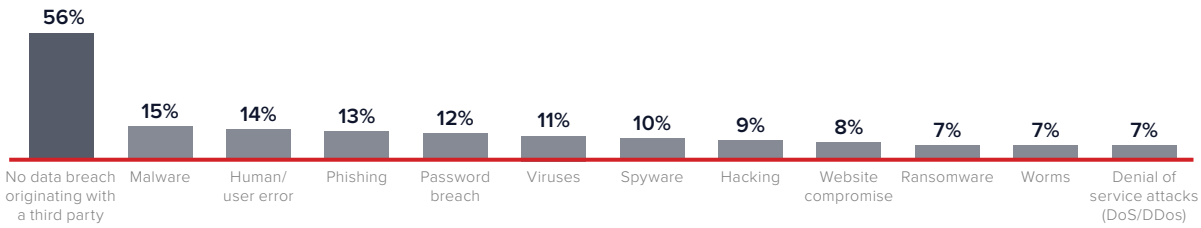
Managing third-party risk is a priority at my org



Key Insight: Most are confident their third-party partners are secure, even though nearly half have experienced a recent third-party data breach which negatively impacted their organization and the third party.

44 percent of respondents have experienced some kind of third-party data breach in the last year. Most breaches were identified within a day by someone other than the third-party partner. Around half discontinued or decreased business conducted with the third party involved in the breach, but most did not change their risk policy as a result.

Third-party breaches in last 12 months



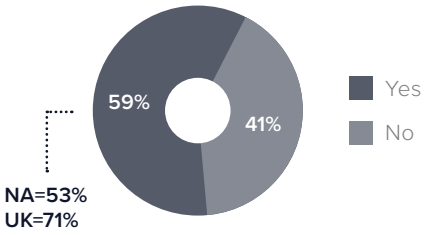
FINDINGS: CURRENT PRACTICES AND SECURITY CONCERNS

While just over half of organizations have formalized third-party data risk management policies in place, most keep an up-to-date inventory of all third parties with whom they share data.

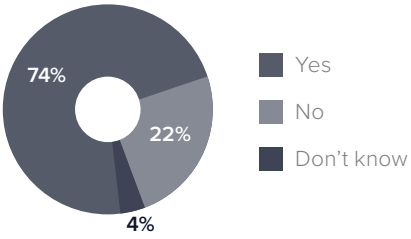
We asked respondents if their organization has a formalized third-party data risk management program or policy. Nearly 60 percent indicated they do have a policy in place. A breakdown of the data shows that larger (500+ employees) companies and U.K. companies are more likely to have formalized policies. With strict data privacy regulations such as GDPR, it is interesting that the percentage for U.K. companies (71 percent) is not higher.

Even though just over half of all respondents have a formal vendor policy in place, 74 percent said that they keep a complete, up-to-date inventory of all third parties with whom they share data. Again, this number was higher amongst larger companies and those located in the U.K. where regulations are more strict.

Third-party data risk management policy in place

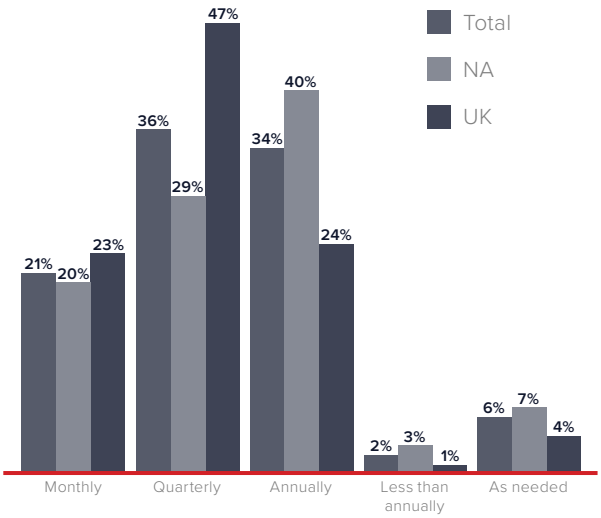


Complete inventory of all third parties with whom share data

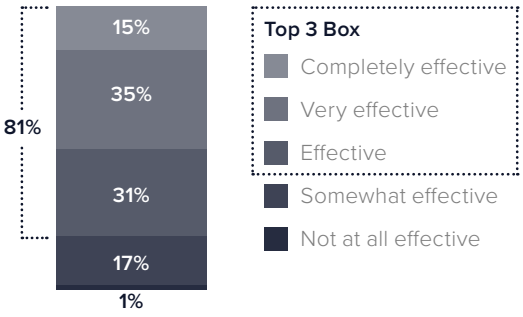


Technology is constantly changing and threats are ever-evolving. Companies must always be on top of the latest attacks trends and adjust policies accordingly. For those with a third-party management policy/program in place, when it comes to how often they are reviewing that policy to ensure that it is up to date and addressing current potential risks, the numbers are reassuring. More than 90 percent review those policies at least annually, with the majority of those doing it more often on a quarterly or monthly basis. 81 percent also feel that the policies they have in place are effective in protecting their organization.

Policy review frequency



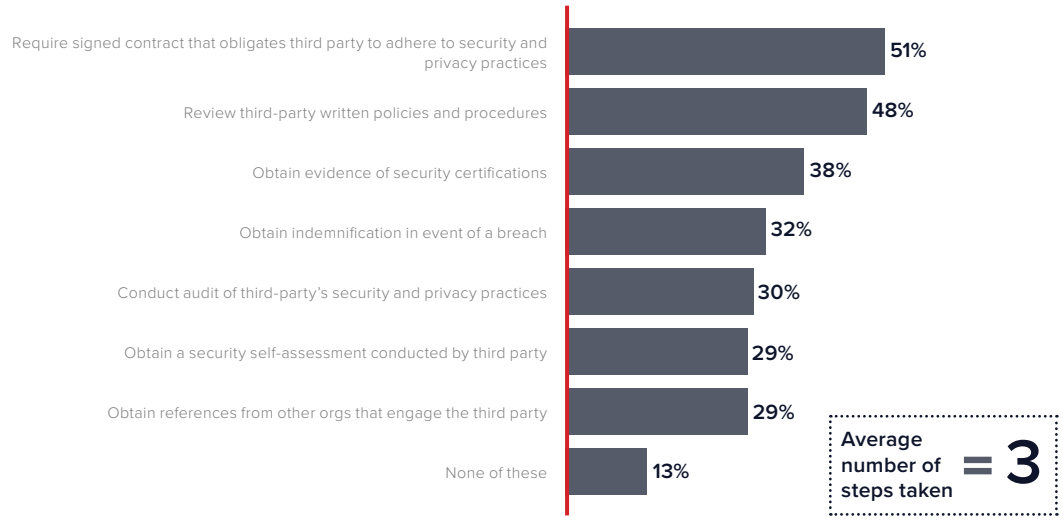
Policy effectiveness rating



HOW WELL ARE COMPANIES EVALUATING THIRD-PARTY POLICIES?

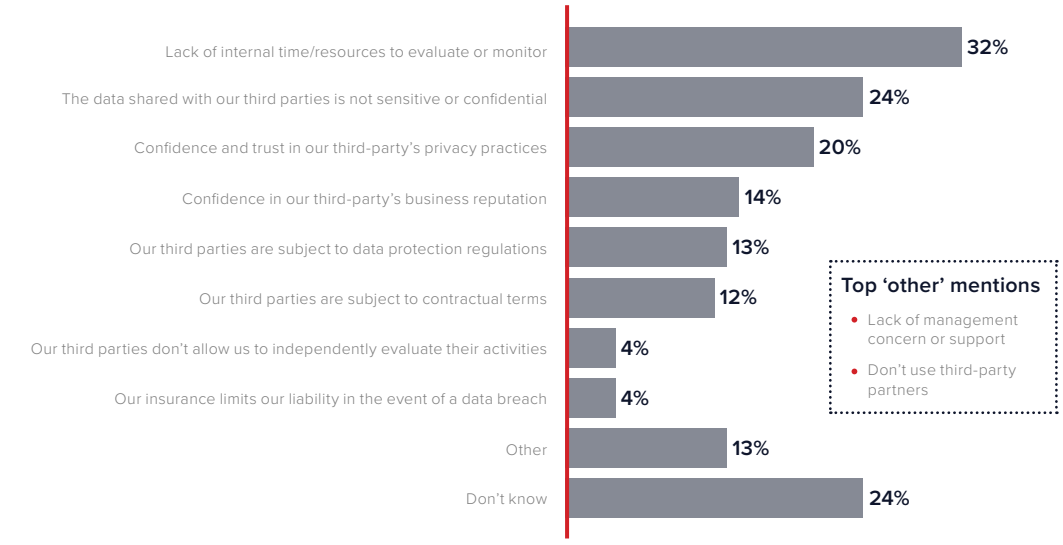
Most organizations take on average three steps to evaluate third-party vendors. We asked respondents which types of steps, if any, they take to evaluate the security and privacy practices of potential vendors before they engage in a business relationship that requires data sharing. Interestingly, only 51 percent require a signed contract that obligates the third party to adhere to security and privacy practices, and just under 50 percent review the written policies of their third parties.

Steps taken to evaluate third-party partners



Thirteen percent of respondents do not take any steps to evaluate their third-party partners, and the top reason companies don't evaluate third parties is due to a lack of time/resources to monitor them. **Twenty percent simply cite "trust" in their vendor's privacy practices as one of the reasons why they do not conduct third-party evaluations.**

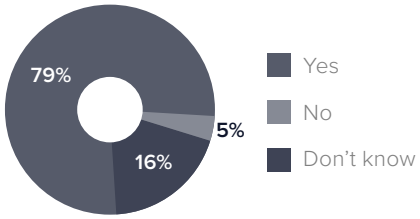
Reasons NOT evaluating third-party partners



Among the steps taken to evaluate third parties, a third of respondents say they obtain indemnification in the event of a breach involving their third party. What does that indemnification look like? Legal and/or monetary consequences for 79 percent of the surveyed companies.

When asked open-endedly what type of penalty they enforce in the case of a violation or breach, our respondents said:

Enforce legal or monetary consequences



- **Contract termination**

  "It would depend on the type of breach of contract but **immediate termination**, seeking refund for lost service, and if those needs are not met then much more severe measures need to be taken like seeking a larger sum and suing for breach of contract."

- **Monetary fine**

  "We would seek what the breach cost us plus **extra damages** to be determined by my company."

- **Lawsuit/legal action**

  "It would have to be judged by law in court."

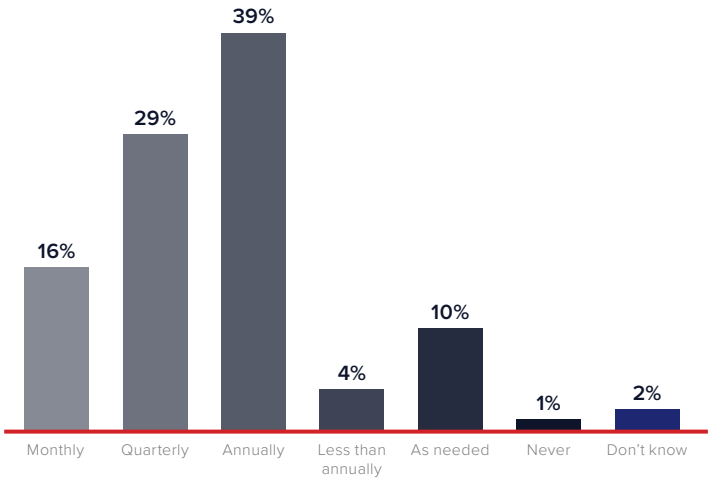
- **Reimbursement of damages**

  "**Cost of loss plus the cost of the fix.**"

  "Any **expenses incurred by our company** as a result of the third-party violation/breach, including technical, legal, and PR expenses."

Amongst respondents who audit their third parties, when asked how frequently they did so, most companies conduct their audits on a quarterly (29 percent) or annual (39 percent) basis. This was most true for larger (500+ employee) companies, with smaller companies more likely to audit on an "as-needed" basis.

Frequency of third-party audits



There are several indicators of potential risk that can be used to audit or evaluate the third parties that companies conduct business with. Some are more obvious, such as:

- History of security incidents or data breaches
- Failed past IT security audits or verifications
- Past legal action taken against them

Others may not be so obvious, but their presence indicates poor business practices that could point to risk when it comes to protecting your company's data:

- Past operational issues or failures
- Complaints/poor reviews from other customers/partners of the third party
- Decline in the quality of the third-party's services
- Past negative PR/media attention involving the third party
- Use of subcontractors (nth parties)

When we asked our respondents which among these they consider to be indicators of potential risk in doing business with their vendors, more than half agreed with the obvious indicators as well as some of the less than obvious ones. **Most notably, the indicator receiving the lowest percentage of response was the use of nth parties, garnering just 41 percent of consideration amongst respondents.**

Indicators of potential risk

THIRD-PARTY RISK IS NOT A TOP PRIORITY

When respondents were asked to rank their agreement with how much they feel third-party risk is a priority at their company, only a third completely agree. When asked why they feel that it is not a priority, they cited:

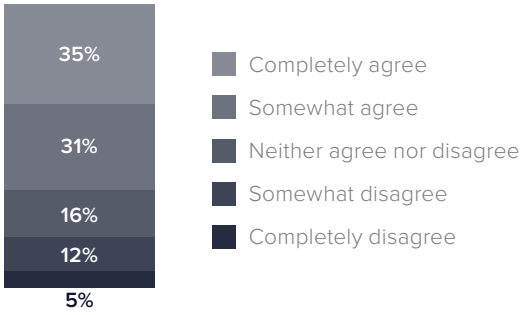
- No senior management support
- Lack of knowledge on how to implement a program
- Lack of resources (time and money)
- Trust in their third parties

Many agree it should be a priority, but that it is not considered important by senior management. Respondents express that they do not have the time, resources, and management understanding to implement a third-party risk management program, nor do they have the knowledge of how to implement one. Companies seem to turn a blind eye, rather than figure out how to deal with the issue of third-party risk and educate senior management on the dangers of not doing so. Respondents even indicted that their history and experience with a third-party vendor provides them with a level of trust that suffices.

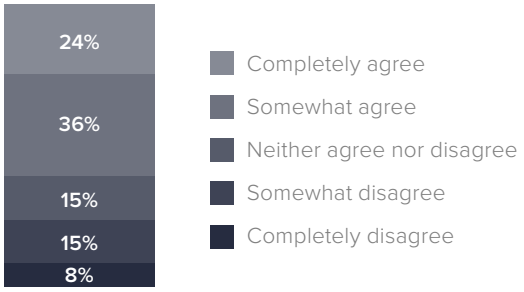
Given what we just learned, it is no surprise that only 24 percent completely agree that their company allocates sufficient resources to managing third-party relationships.

And remember those nth parties? The ones that less than half of respondents considered an indicator of risk? Only 28 percent of respondents were confident that their third parties notified them when they shared their data with nth parties.

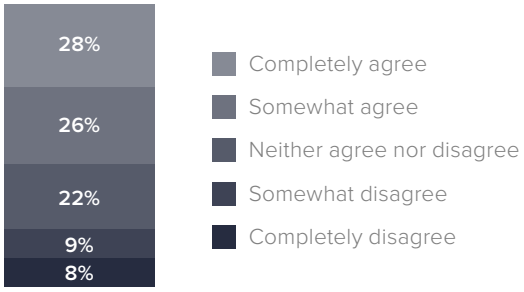
Managing third-party relationship risk is a priority at my organization



My org allocates sufficient resources to managing third-party relationships



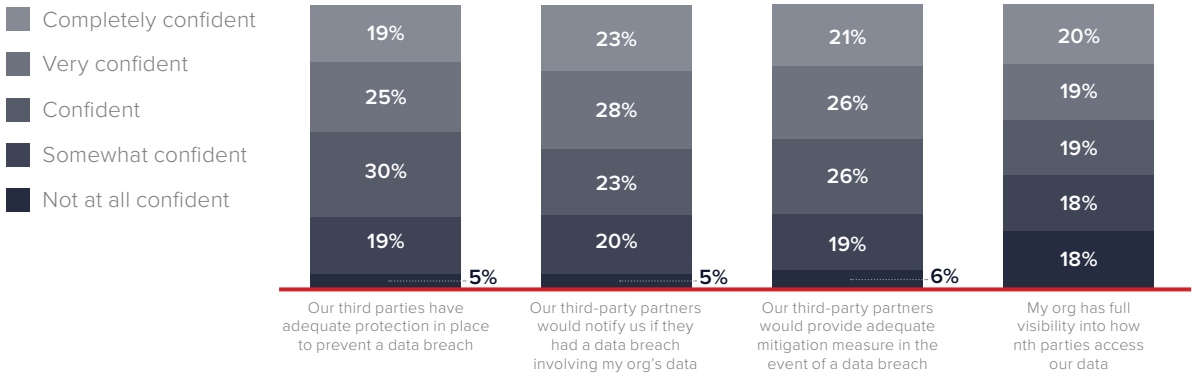
Our third-party partners notify us when my org's data is shared with further parties



TRUSTED PARTNERS

Overall, most feel confident that third-party partners have adequate protection and would provide sufficient communication and mitigation measures in the event of a breach. Three quarters of respondents are confident that their third parties have adequate protection in place in order to prevent a data breach, and that their third parties would notify them if there was a breach involving their data. Remember that latter one. We'll get back to that later. Three quarters are also confident that their third parties would provide adequate mitigation measures in the event of a breach.

Confidence level in third-party partners

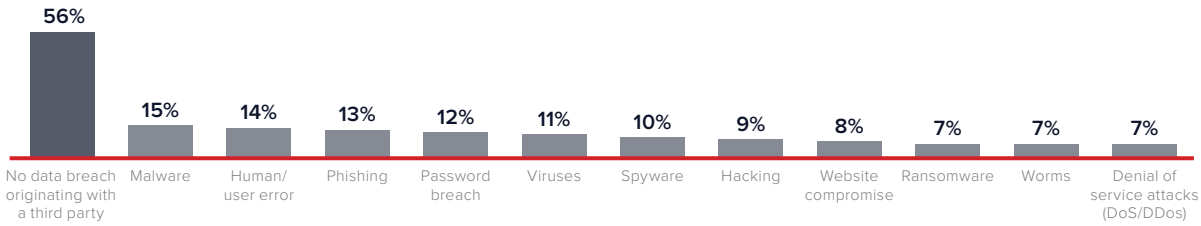


The last confidence measure the survey covered was in regard to how much visibility the responding company had into how nth parties accessed their data. In this case, confidence was a bit lower than with the other criteria, however still strong with roughly 60 percent of respondents feeling confident that they had full visibility into how nth parties access their data. This is particularly notable when only 28 percent indicated earlier that they were confident that their third parties notified them when sharing their data with nth parties.

WHEN A BREACH OCCURS

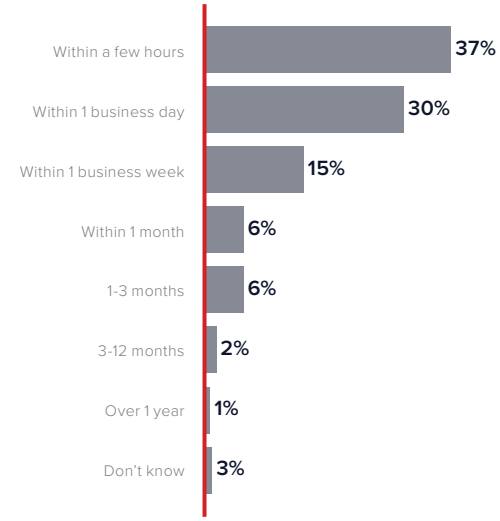
Respondents were asked if they had experienced a breach through a given list of means in the past 12 months that had originated with a third party. Just under half of respondents indicated that they had experienced a third-party data breach in the last year.

Third-party breaches in last 12 months

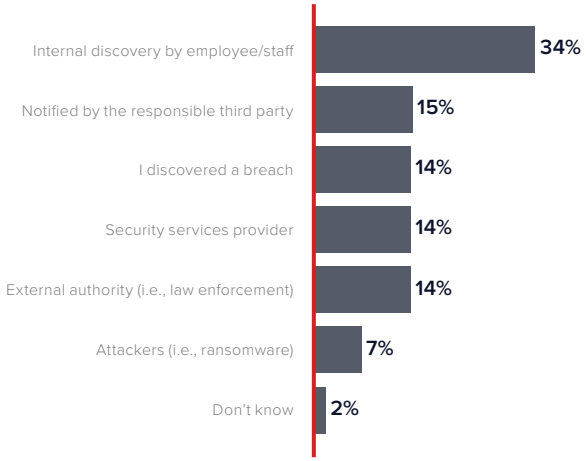


Additional questions revealed that most of the breaches were identified within a day, but the really interesting information is *who* discovered the breach. Remember that point from earlier that three quarters of respondents were confident that third parties would notify them if there was a breach involving their data? **When a breach did occur, only 15 percent reported that they were notified of the breach by the responsible third party.**

How quickly breach was identified



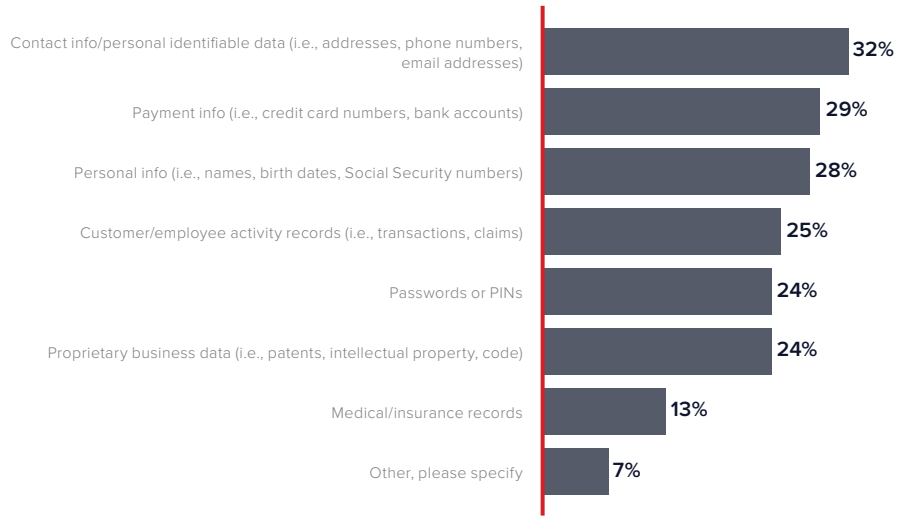
Who discovered breach



Of the 241 respondents who experienced a breach related to a third party in the last year, personal identifiable data (32 percent) and payment info (29 percent) are the data that was most often affected by the breach, causing reduced productivity, increased operational complexity, higher security costs and system downtime.

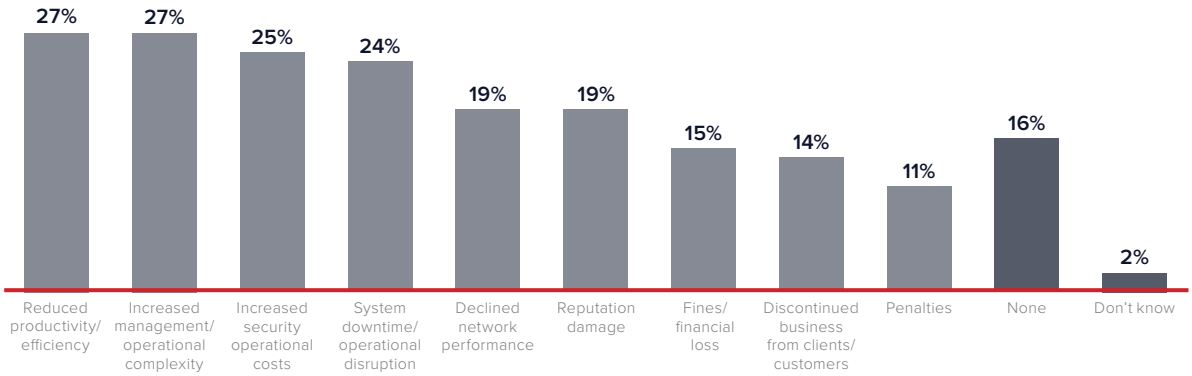
Contact information (i.e. addresses, phone numbers, etc.) was obtained 32 percent of the time, while credit card numbers and bank accounts were exposed in 29 percent of the breaches that occurred. Passwords and PINs, and proprietary business data (i.e. intellectual property and patents) were obtained in a quarter of the breaches.

Data affected by third-party breaches



When a company experiences a breach, the reputational damage will not be lessened by knowledge that the breach was caused by a third party. Nineteen percent of respondents learned that the hard way. The third-party breaches resulted in discontinued business most often for larger organizations, with 14 percent of overall respondents experiencing this consequence. A quarter of respondents reported reduced productivity, increased operational complexity and security costs, and operational disruption (downtime).

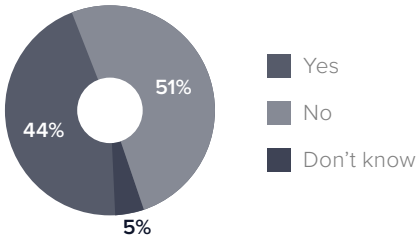
Effect of third-party breach



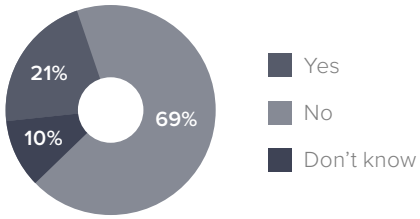
AFTER THE BREACH

Around 44 percent of respondents discontinued or decreased business conducted with the third party involved in the breach. Not only did a solid 51 percent continue to do business with the third party after the breach, most (69 percent) did not change their risk policy as a result. North American companies were more likely to make changes to their risk policy after a breach.

Discontinued or decreased business with third party



Changed third-party risk practices



CONCLUSION

The results of the survey reinforced the initial assumption that companies fail to recognize and make third-party risk management a priority, and nth-party risk even less so. Senior management is rightfully focused on business operations, however evidence from the survey shows it could be detrimental not to apply greater consideration and resources to mitigate the potential impact a breach involving the company's third- and nth-parties presents. Many organizations continue to feel that if their company has internal policies and controls in place, that their data is safe. The fact that just under half of the companies surveyed experienced a breach due to a third party proves otherwise. As digital transformation and the rapid competitive environment continue to pressure expansion of third parties to achieve business objectives, potential risk, especially nth parties, will continue to escalate. Increasing regulatory requirements and greater potential impact from violations in combination with third-party expansion will result is a recipe for escalating and uncontrollable risk. Readers of this report are encouraged to conduct a third-party risk assessment that not only identifies third and nth parties, but develops risk rankings based on potential business impact and regulatory ramifications.

eSentire is the largest pure-play Managed Detection and Response (MDR) service provider, keeping organizations safe from constantly evolving cyberattacks that technology alone cannot prevent. Its 24x7 Security Operations Center (SOC), staffed by elite security analysts, hunts, investigates, and responds in real-time to known and unknown threats before they become business-disrupting events. Protecting more than $6 trillion in corporate assets, eSentire absorbs the complexity of cybersecurity, delivering enterprise-grade protection and the ability to comply with growing regulatory requirements. For more information, visit **www.eSentire.com** and follow **@eSentire**.