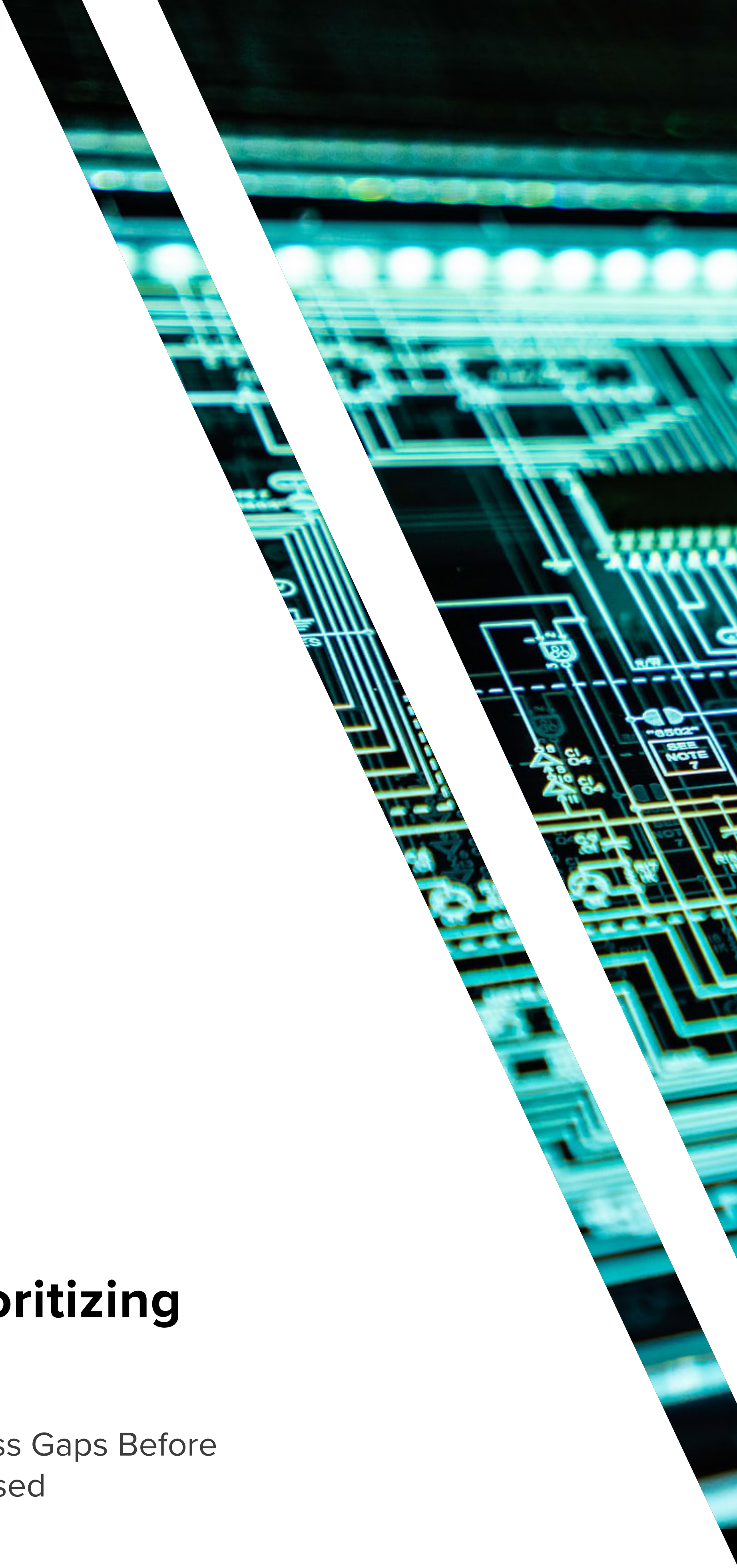
FORRESTER®



Why Isn't Your Organization Prioritizing Third-Party Risk?

How To Address Key Process Gaps Before Your Business Is Compromised

Table of Contents

Project Director:
Megan Doerr,
Market Impact Consultant

Contributing Research:
Forrester's Security & Risk research group

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

Executive Summary

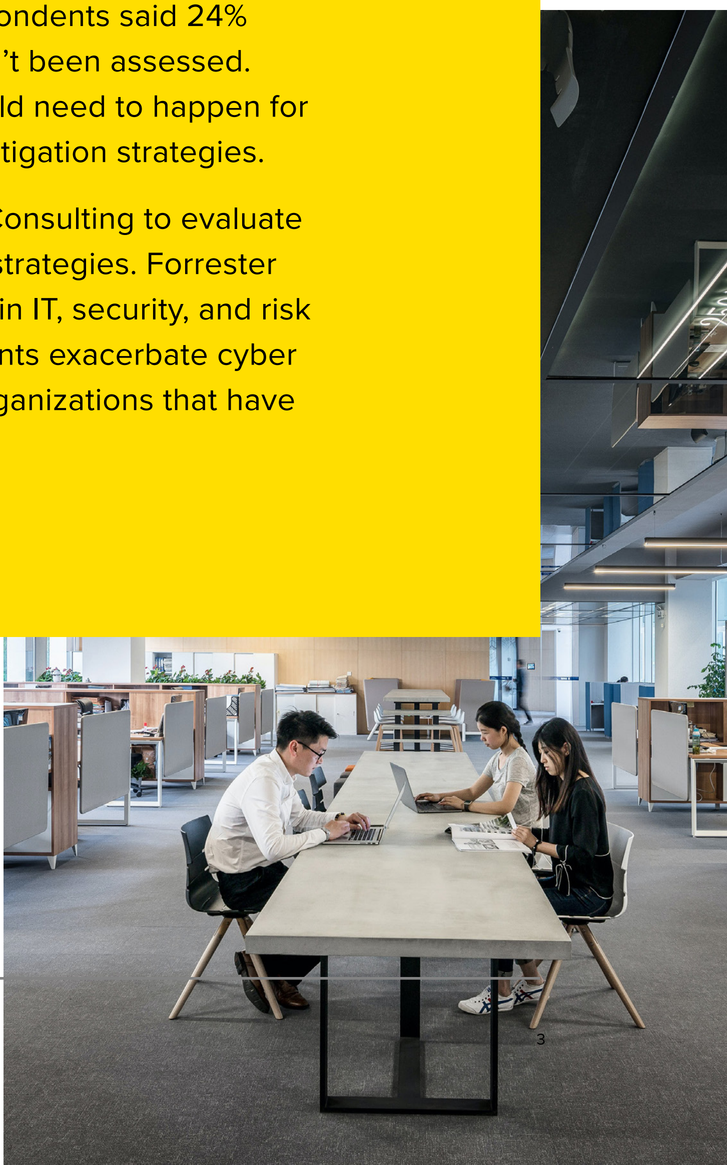
All information that flows through an enterprise presents a security risk. Yet in stratifying enterprise risk, many operations teams tend to deprioritize third-party connections as a potential breach source. This is understandable, since trust is a core principle of partnerships. We expect vendors to meet our standards and have our best interests at heart.

Third parties fail to measure up to these expectations, though. Two-thirds of survey respondents reported that their organizations experienced a third-party cyber incident in the past year. And even though 82% recognized that third-party threats exposed their organizations to risk, many failed — and continue to fail — to take adequate mitigation measures. Only half of respondents reported their organizations actively prioritize such risks, even as the percentage of data shared with third parties will ramp up over the next five years (from 30%-41% by 2026).

While most enterprises have adopted third-party risk management tools, vendor assessment practices are hit or miss. Respondents said 24% of new vendors and 40% of current vendors haven't been assessed. Respondents indicated that significant events would need to happen for their organizations to elevate the importance of mitigation strategies.

In May 2021, CyberGRX commissioned Forrester Consulting to evaluate organizations' third-party cyber risk management strategies. Forrester conducted an online survey with 319 respondents in IT, security, and risk roles to explore this topic. We found that weak points exacerbate cyber threats. We highlight the mitigation practices of organizations that have avoided third-party cyber risk incidents.

Key Findings →



Key Findings

Today's organizations constantly exchange confidential information with third parties. This exposes both sides to significant cyber risk. These information supply lines enabled by clouds and software-as-a-service (SaaS) are expected to grow in importance for many enterprises. In the next five years, organizations estimate sharing 41% of critical data with third parties.

Current third-party risk prevention strategies leave organizations vulnerable. The breakdown between businesses and their third-parties is due to a lack of prioritization and a matter of approach. Ninety-five percent of respondents said their organizations experienced a strategy- or technology-based challenge in managing third-party risk. Without proper oversight, companies become vulnerable to cybersecurity threats, including data loss and ransomware.

Organizations stung by third-party cyber incidents tend to ignore safe risk management practices. Organizations with a third-party cyber incident express a higher level of concern about managing such risks. However, organizations with an incident also tend to share a higher percentage of their critical data (30%) than firms that haven't been hit (22%). And firms with an incident are less likely to have tools in place to mitigate third-party cyber risks.

Mitigating third-party risk requires a different approach to strategy and technology. Organizations need to approach third-party risk with a new holistic, ecosystem-focused, and cybersecurity-focused strategic mindset. This includes updated third-party assessment analysis, standardized processes, and higher-quality technology solutions.

Organizations Rely On Third Parties And Risk Is An Afterthought

Though the security field is rapidly assimilating promising technologies, such as machine learning and analytics, cyber incidents are not going away. In fact, they're more prominent and dangerous than ever. A certain amount of risk is inevitable and necessary to conduct business in a world that is still highly reliant upon trust. But, with the average cost of a data breach totaling $3.86 million, organizations can no longer afford to ignore such a glaring issue.[1]

Third-party cyber risk incidents are costly and often avoidable. Organizations that fail to take thoughtful steps to monitor, defend, and prepare for third-party cyber incidents undermine their cybersecurity posture. But how do organizations know what to do and if their strategy for controlling these risks is robust enough to keep them safe?

82%

said third-party threats present the most significant risk for exposure. Even though many organizations recognize the hazards posed by third parties, their actions don't reflect effective mitigation.

In surveying 319 IT security and risk management decision-makers, we found that 82% said third-party threats present the most significant risk for exposure. Even though many organizations recognize the hazards posed by third parties, their actions don't reflect effective mitigation. We also found that:

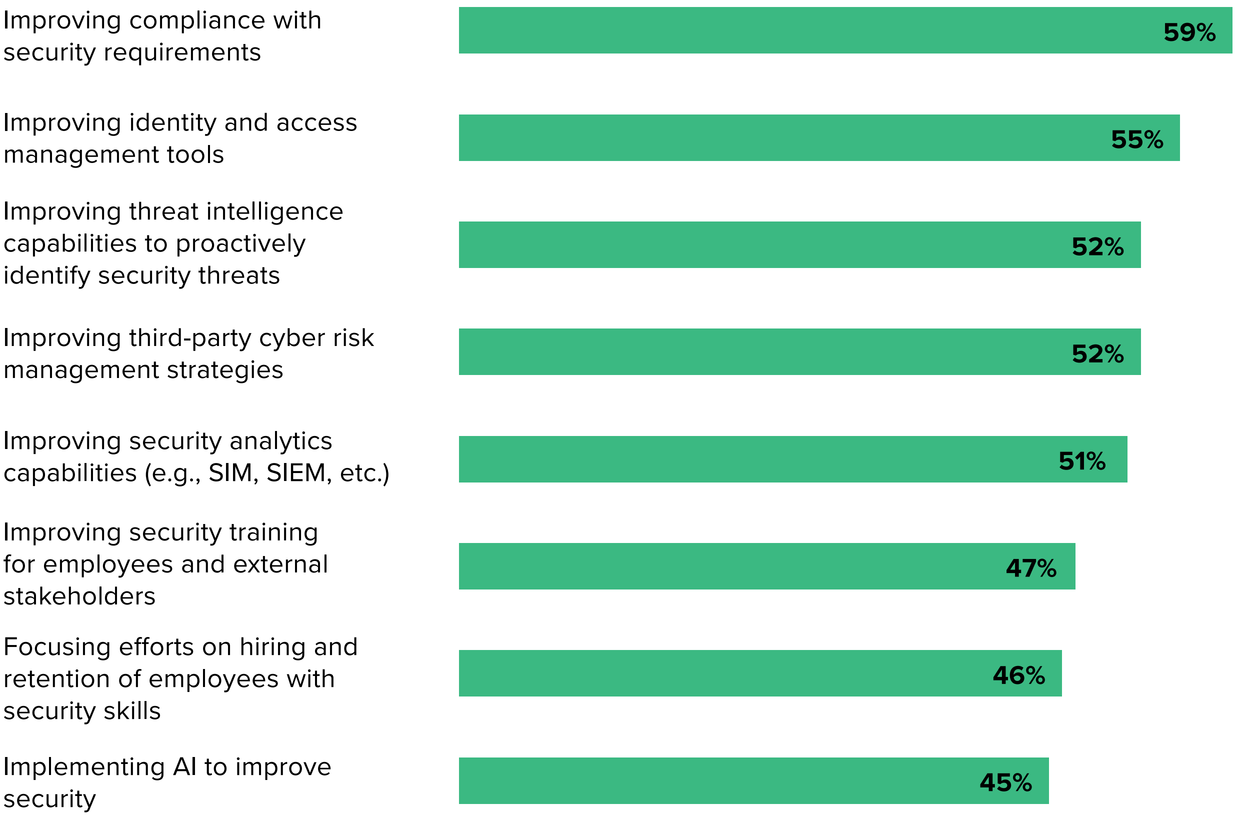
- **Less than half of organizations actively prioritize third-party risk management strategies.** While organizations proactively update their own security practices, only about half of respondents said their organizations consciously make improvements to the way they manage third-party risks (see Figure 1). Lacking a defined third-party risk management strategy creates the opportunity for a breach, even if internal risk management strategies are otherwise solid and effective.
- **Organizations share large amounts of critical data with third parties.** As if hackers needed more reason to attack, respondents reported

sharing almost a third of their organization's critical data, which is data that's considered essential to the organization's mission, with various third parties. Critical data may include customer information, sales data, or other forms of intellectual property. The percentage is expected to rise to 41% over the next five years, which makes prioritizing third-party risk even more important to prevent data from falling into the wrong hands.

> Lacking a defined third-party risk management strategy creates the opportunity for a breach, even if internal risk management strategies are otherwise solid and effective.

Figure 1

"What are your organization's top security priorities over the next 12 months?"

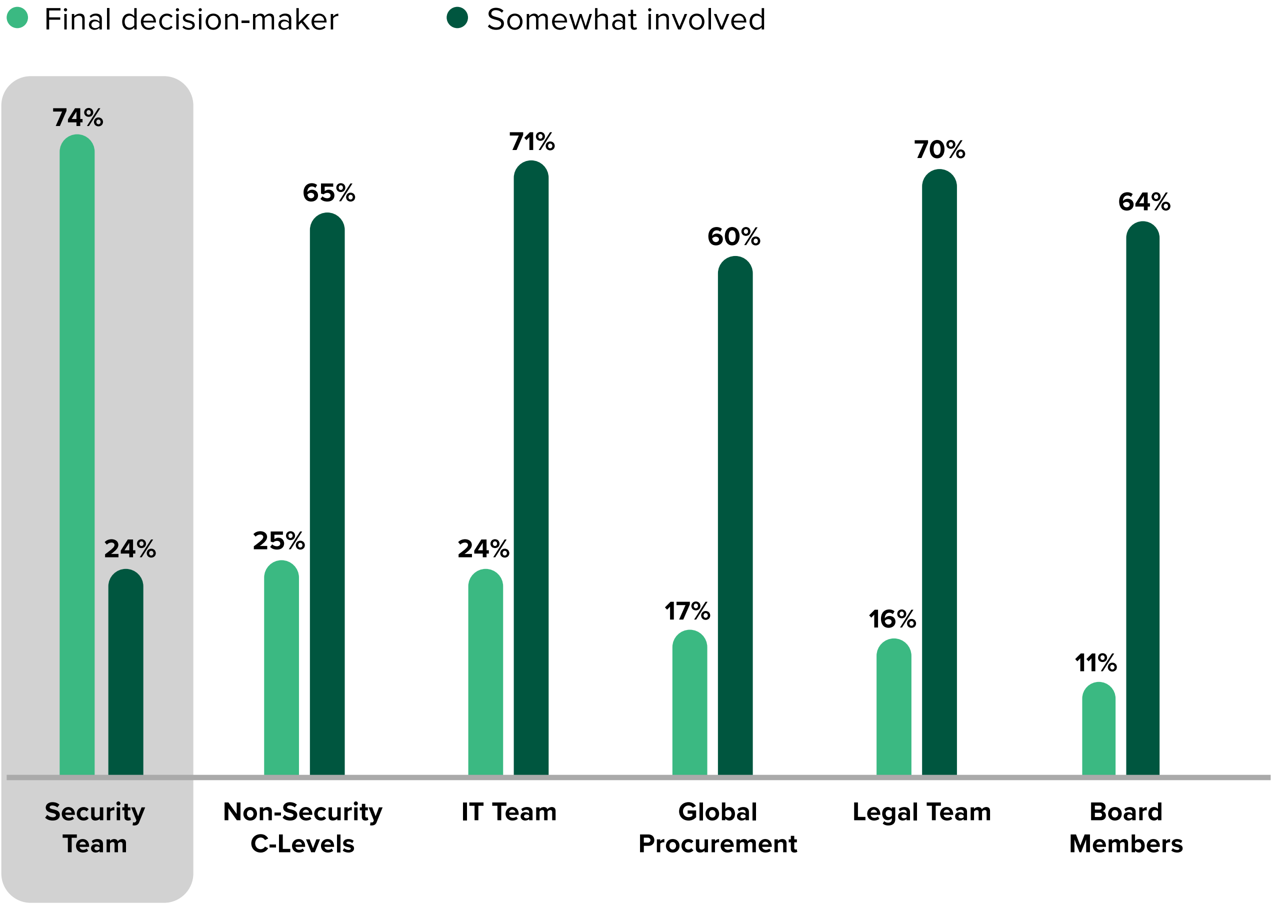


Base: 319 global IT security and risk management decision-makers
Note: Showing top 8 responses
Source: A commissioned study conducted by Forrester Consulting on behalf of CyberGRX, May 2021

- **Third-party cyber risk strategies involve too many teams that lack understanding.** While 74% of respondents reported their organizations' security teams as the final decision-makers for third-party cyber risk management strategies, other business teams have high levels of involvement (see Figure 2). Nearly three-quarters (74%) of decision-makers reported that non-security business leaders have at best an intermediate understanding of third-party cyber risk management. Yet organizations that have experienced third-party risk incidents have often asked non-security C-level executives to manage their third-party cyber-risk management strategy.

Figure 2

"How involved are each of the following stakeholders in third-party cyber risk management strategy creation at your organization?"



Base: 319 global IT security and risk management decision-makers
Source: A commissioned study conducted by Forrester Consulting on behalf of CyberGRX, May 2021

Misdirected Strategy Undermines Business Performance

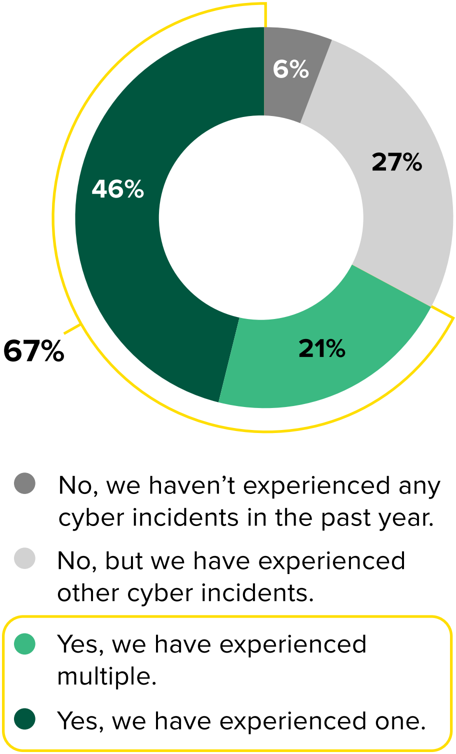
Risk is rampant. Two-thirds of decision-makers reported their organizations have experienced a third-party risk incident in the past year (see Figure 3). Sixty-three percent of respondents whose organizations have been hit stated that third-party relationships expose their organizations to critical security vulnerabilities. But, if organizations understand the importance of risk, why is it still so difficult to manage — or at least prioritize? Ninety-five percent of respondents reported that their organizations' third-party risk management efforts are impeded by poor collaboration, inefficient classification, and a lack of strategic guidance (see Figure 4).

Our survey uncovered four main weaknesses with third-party risk management strategies:

- Third-party threats are thought of differently than all other risks.
- Key foundational security hygiene protocols are only taken post-risk instead of as a preventive measure.
- Current risk management strategies, tools, and technologies lack functional necessities.
- Vendor assessments are subpar and lack results that provide a complete view of third-party risk.

Figure 3

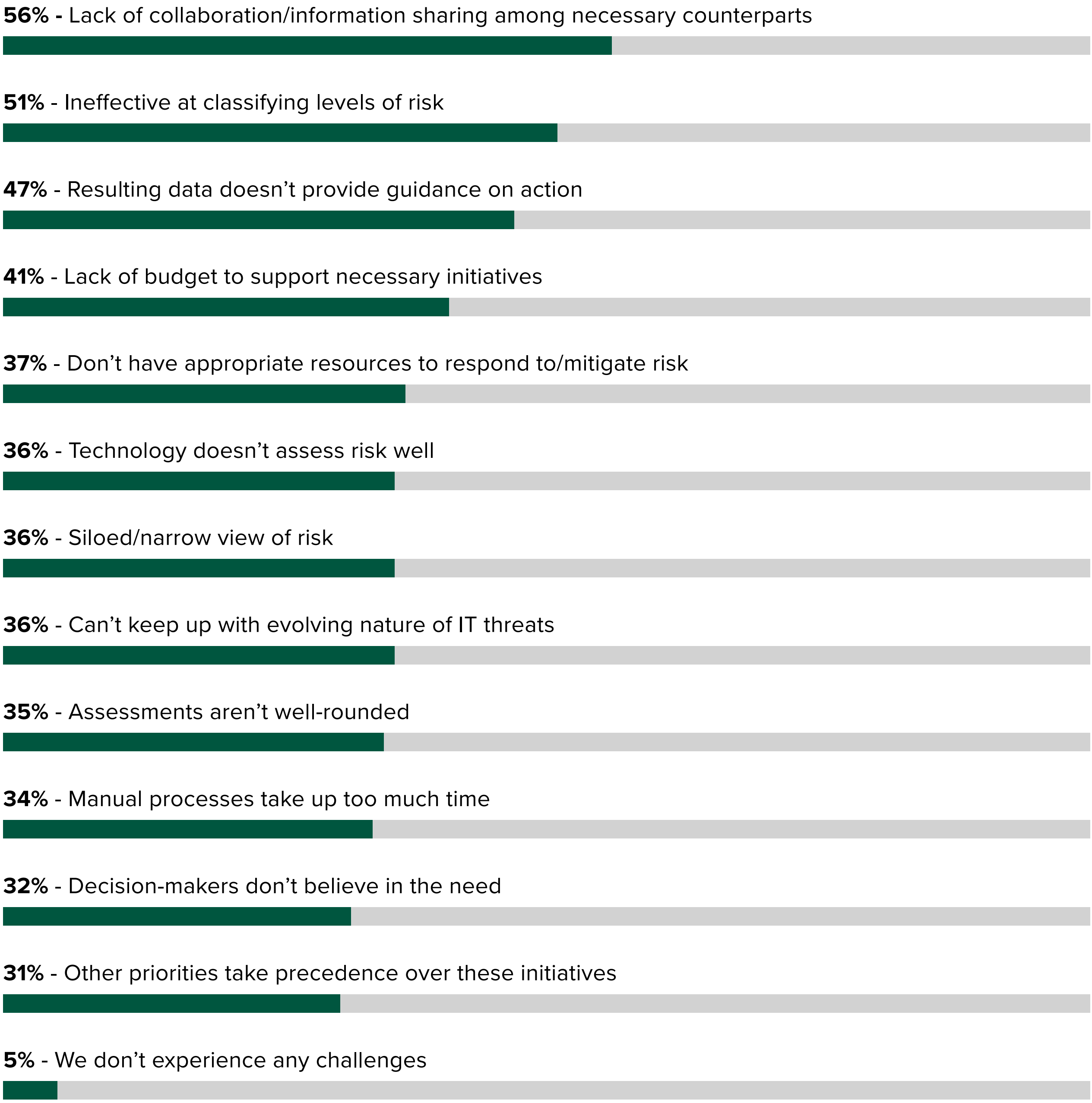
"Has your organization experienced a third-party risk incident in the past year?"



Base: 319 global IT security and risk management decision-makers
Source: A commissioned study conducted by Forrester Consulting on behalf of CyberGRX, May 2021

Figure 4

“Which of the following obstacles prevent your organization from best managing its third-party risk?”



Base: 319 Global IT security and risk management decision-makers
Source: A commissioned study conducted by Forrester Consulting on behalf of CyberGRX, May 2021

THIRD-PARTY THREATS ARE UNACCOUNTED FOR

In general, organizations are aware of and understand the various entry points of risk (see Figure 5). Even though many are prepared to face these threats from internal sources, many of these risks, such as ransomware/extortionware, data breaches, malware, phishing, and distributed denial of service attacks (DDoS), are often borne from third-party activity. By confining third-party risk to its own bucket, rather than focusing on the similarities of third- and first-party risks, organizations lose out on a more significant understanding of the security ecosystem and how to mobilize vendor relationships to prevent risk.

Figure 5

"How concerning are the following risks to your organization?"

(Showing "Concerning" and "Highly concerning")

89%
Data breach

83%
Theft of data, IP, or equipment containing sensitive data

80%
Malware

73%
Fraud

69%
Email-based phishing attack

66%
Denial of service attack

61%
Third-party/ supplier risk

59%
Malicious insider

44%
Geopolitical risk

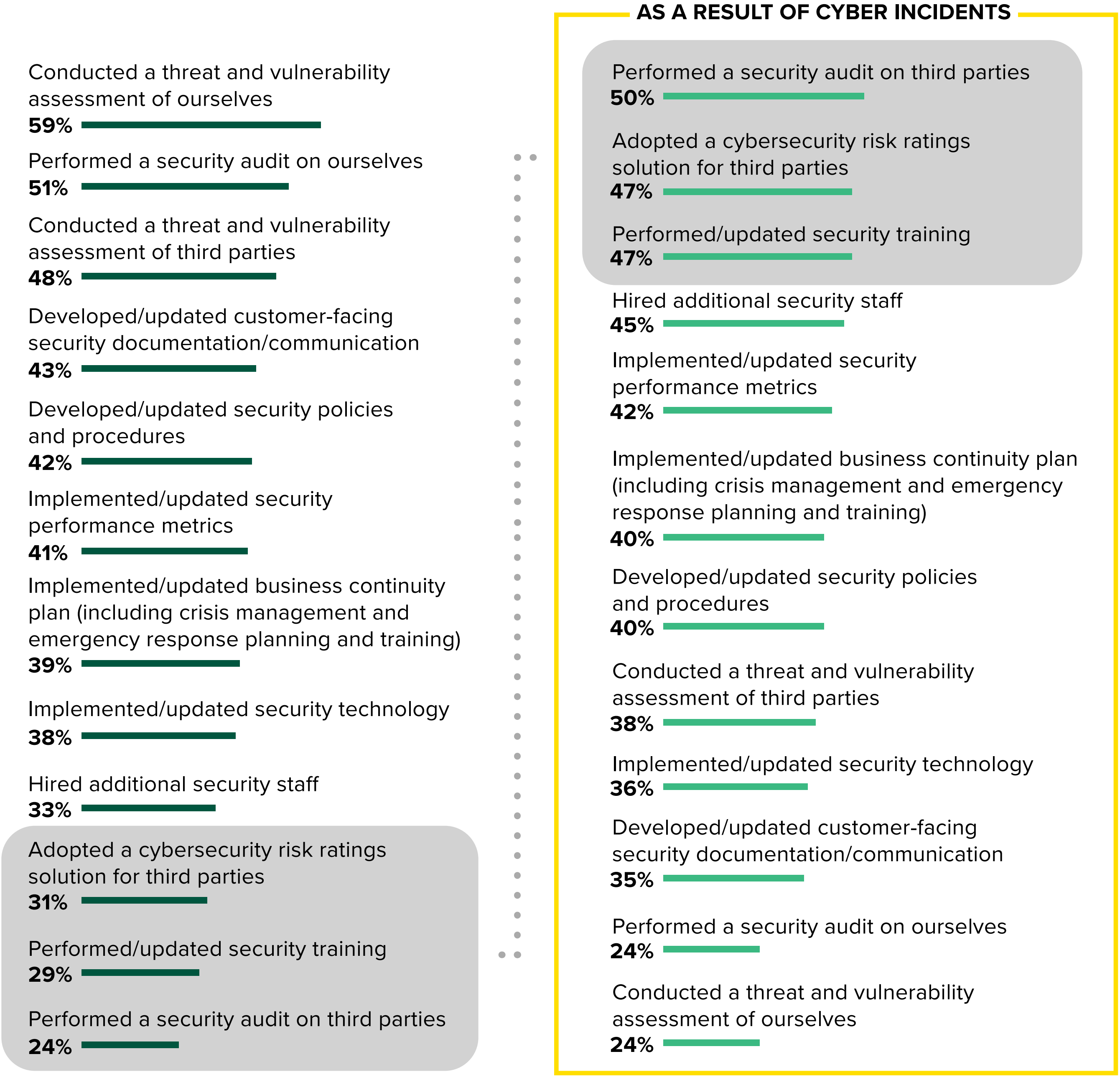
Base: 319 global IT security and risk management decision-makers
Source: A commissioned study conducted by Forrester Consulting on behalf of CyberGRX, May 2021

SECURITY HYGIENE PROTOCOLS MISS THE MARK

Both routine security hygiene protocols and actions taken due to incidents are imperative to an organization's cybersecurity risk posture. However, most organizations appear to strengthen key facets of cybersecurity only after an incident occurs. As with physical health, prevention is the best solution for cybersecurity health. Assessments, audits, training, and risk rating solutions aren't currently part of standard security hygiene protocols, even though they should be (see Figure 6). When these actions only occur when problems arise, the lack of preparedness adds to an enterprise's risk.

Figure 6

“Which of these actions are part of your regular security program, and which were taken as a result of cyber incidents in the past year?”



Organizations are **2x** as likely to perform a third-party security audit AFTER they experience a cyber incident.

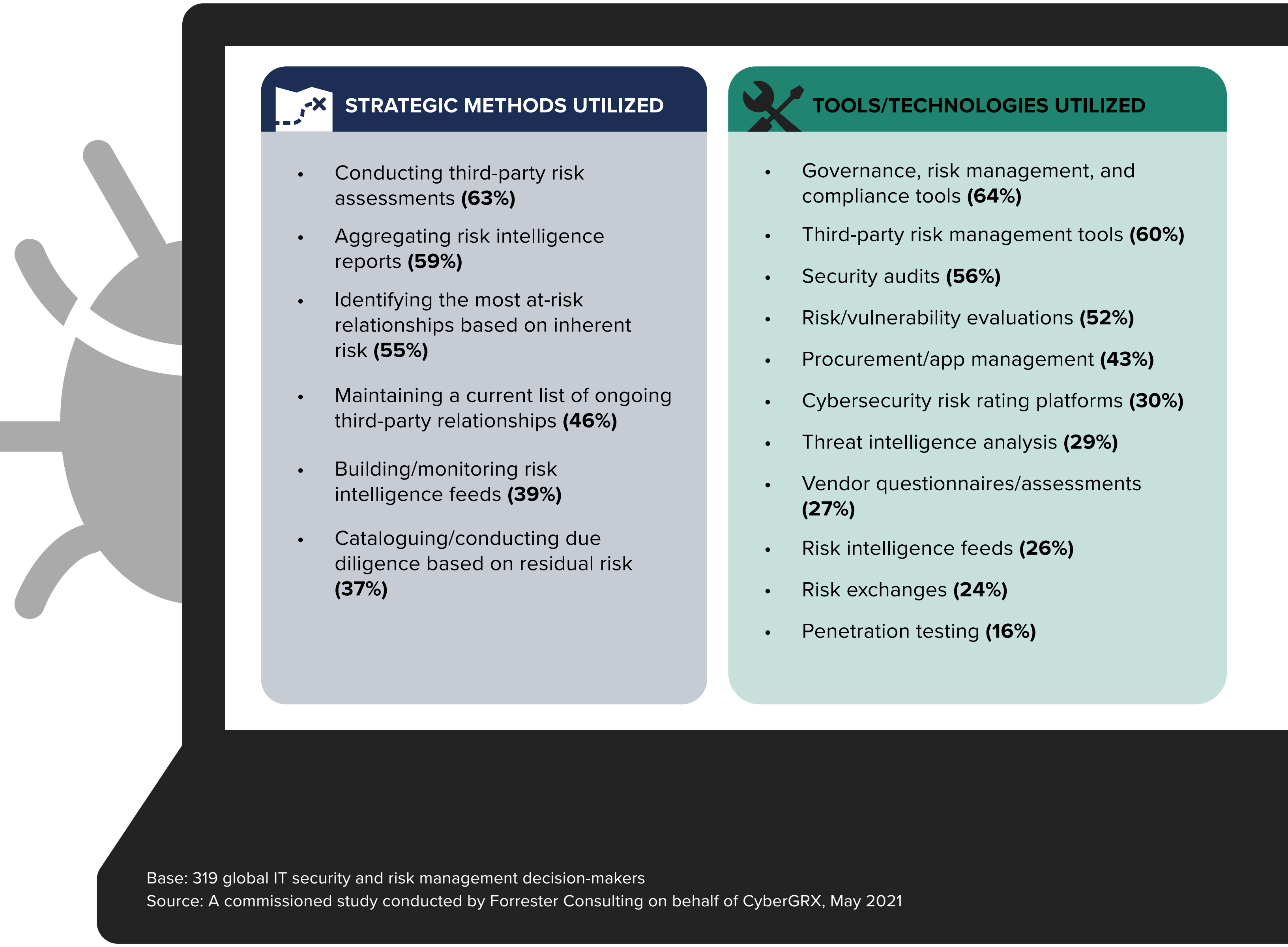
Base: 300 Global IT security and risk management decision-makers
Source: A commissioned study conducted by Forrester Consulting on behalf of CyberGRX, May 2021

THIRD-PARTY STRATEGIES AND TECHNOLOGIES ARE INADEQUATE

Organizations’ third-party cyber risk management strategies include a varied set of methods and technologies (see Figure 7). While more than half of respondents are actively conducting third-party risk assessments, aggregating risk intelligence reports, and identifying at-risk relationships, most organizations have yet to implement practical functions such as risk intelligence feeds or routine due diligence.

Figure 7

Current Strategies And Technologies Present Opportunity For Threats



STRATEGIC METHODS UTILIZED

- Conducting third-party risk assessments **(63%)**
- Aggregating risk intelligence reports **(59%)**
- Identifying the most at-risk relationships based on inherent risk **(55%)**
- Maintaining a current list of ongoing third-party relationships **(46%)**
- Building/monitoring risk intelligence feeds **(39%)**
- Cataloguing/conducting due diligence based on residual risk **(37%)**

TOOLS/TECHNOLOGIES UTILIZED

- Governance, risk management, and compliance tools **(64%)**
- Third-party risk management tools **(60%)**
- Security audits **(56%)**
- Risk/vulnerability evaluations **(52%)**
- Procurement/app management **(43%)**
- Cybersecurity risk rating platforms **(30%)**
- Threat intelligence analysis **(29%)**
- Vendor questionnaires/assessments **(27%)**
- Risk intelligence feeds **(26%)**
- Risk exchanges **(24%)**
- Penetration testing **(16%)**

Base: 319 global IT security and risk management decision-makers
Source: A commissioned study conducted by Forrester Consulting on behalf of CyberGRX, May 2021

On the technology side, many organizations utilize governance, risk management, and compliance (GRC) tools, third-party cyber risk management tools, and security audits. Yet the key technologies to help identify and mitigate risk — penetration testing, vendor assessments, and threat intelligence analysis, to name a few — are less popular.

Testing annually through a survey or managing third-party compliance by contract is insufficient.

Inefficient processes often yield poor results, and it's insufficient to test annually through a survey and manage your third-party's compliance by contract. Infrequent monitoring means organizations are unlikely to thoroughly understand what is going on with their third parties. All companies are in a constant state of flux, meaning change within the third party translates to a change in risk levels for the first party. These subpar strategies put organizations at risk of needing additional security/audit requirements (66%), increased spending to resolve issues (37%), and difficulty attracting new customers (25%).

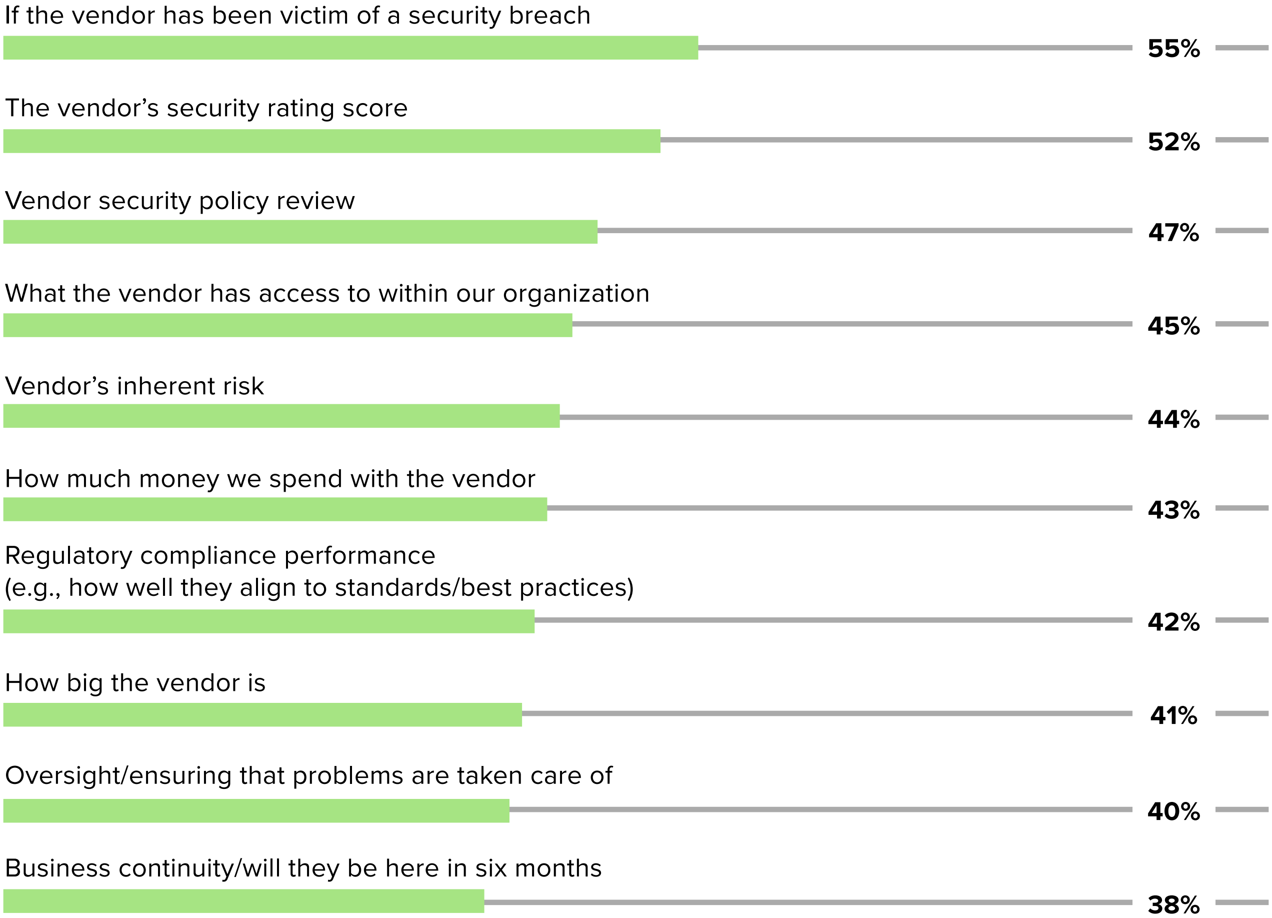
MANUAL VENDOR ASSESSMENTS DON'T PROVIDE AN ADEQUATE VIEW OF THIRD PARTIES

Organizations struggle to manage third-party risk programs for various reasons, but one of the main challenges is a slow and cumbersome assessment process. Assessments are typically lengthy to complete and often lack the critical information necessary to make a sound decision on vendor suitability. These factors delay assessments or cause poor-quality judgments. As a result, respondents reported that, on average, approximately 24% of new vendors and 40% of current vendors remain unassessed. And, even when performing these assessments, the organizations only skim the surface of defining the level of risk, leaving out critical components of accurate risk assessment (see Figure 8).

Perhaps even more concerning is that only 46% of respondents said their organizations suspend risky third-party relationships until an issue is resolved. **Annual assessments are a check box for compliance but not a viable solution for continual management of third-party risks.** More needs to happen to better manage third-party cybersecurity risks.

Figure 8

Factors Used To Evaluate Level Of Risk Exposure



Base: 319 global IT security and risk management decision-makers
Source: A commissioned study conducted by Forrester Consulting on behalf of CyberGRX, May 2021

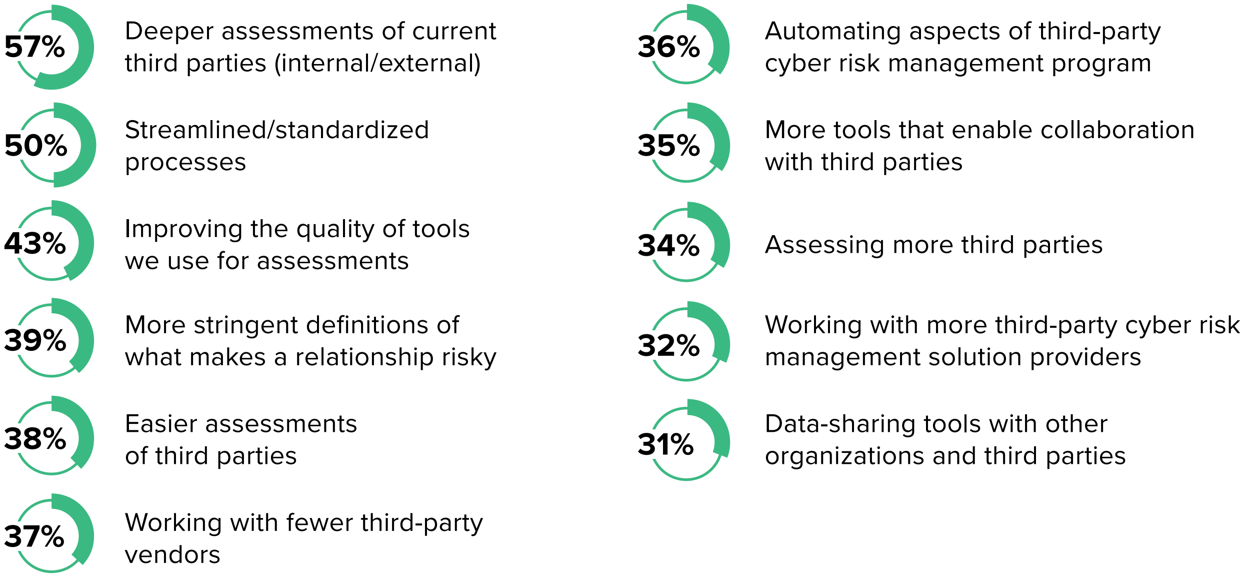
Mitigating Third-Party Cyber Risks Improves Business And Customer Experience

The good news is that organizations aren't just sitting ducks; many have taken action to improve their third-party cyber risk management strategies. Sixty percent of respondents said their organizations are currently making improvements to these strategies today. Yet to fully negate the four factors of problematic strategies, these improvements must be thoughtful and actionable.

The right solution doesn't just check a bunch of boxes for the sake of compliance; it provides a thoughtful approach that includes a **portfolio-wide view** to spot third-party weaknesses (see Figure 9). Organizations should consider deeper third-party assessment analysis, standardized processes, and improving the quality of tools used. Implementing these changes helps organizations improve the quality of their third-party risk management programs, strengthening their ability to prevent and respond to threats.

Figure 9

"What solutions would strengthen your third-party cyber risk management strategy and prevent future risk?"



Base: 319 global IT security and risk management decision-makers
Source: A commissioned study conducted by Forrester Consulting on behalf of CyberGRX, May 2021

These improvements will ultimately lead to significant business benefits for organizations. In fact, 100% of respondents reported anticipating business and customer benefits from a more robust third-party cyber risk management strategy (see Figure 10). Strategy improvements can lead to internal benefits, such as a better understanding of risk and an improved ability to assess risk, while also benefiting the end customer and the organization's ability to innovate and thrive.

Figure 10

Benefits Of A Stronger Third-Party Cyber Risk Management Strategy

61% Better understanding of enterprise risk across siloes

49% Improved ability to assess risk

43% Better innovation

56% Increased trust from customers

47% Fewer security incidents

37% Increased revenue

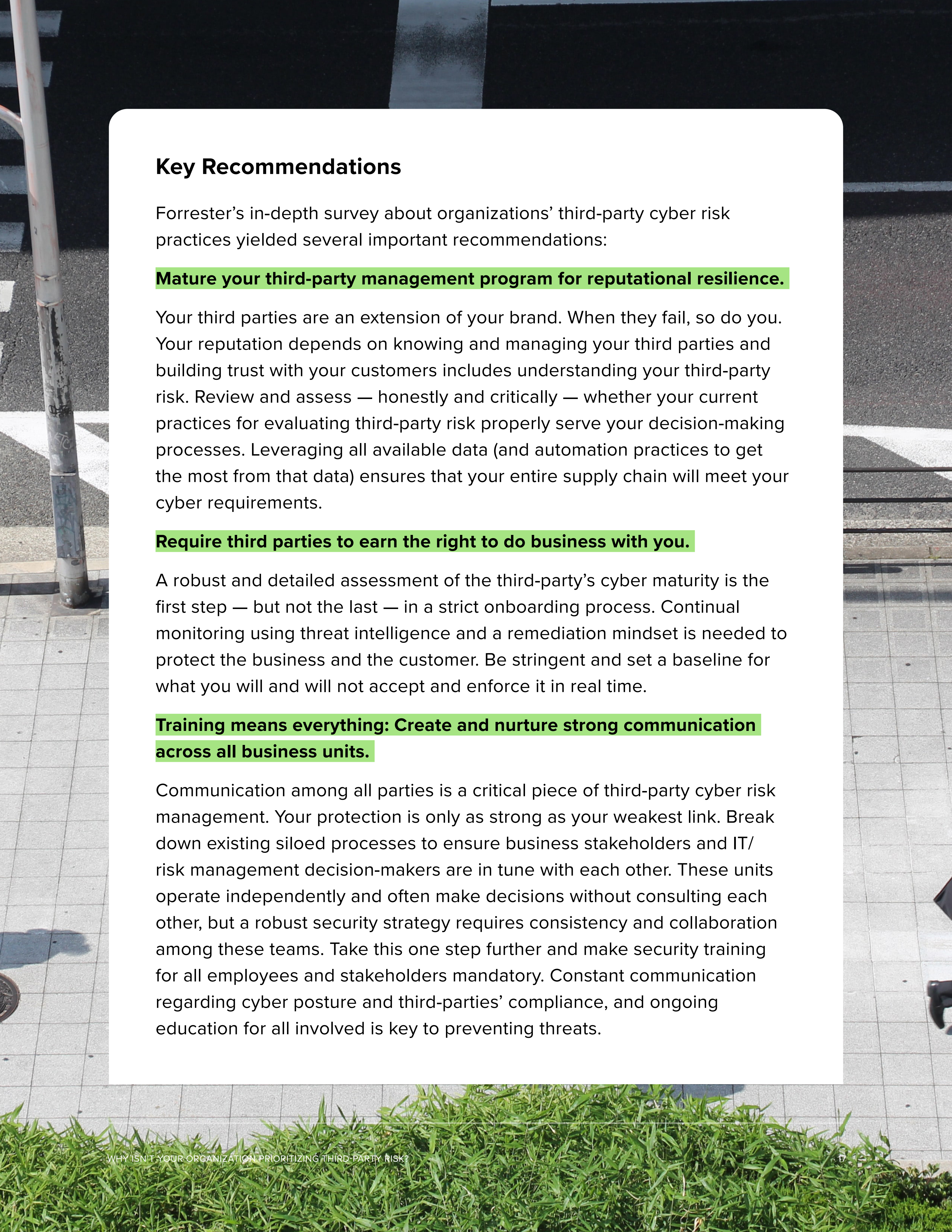
51% Improved customer experience

45% Faster risk assessment

37% Improved employee experience

Base: 319 global IT security and risk management decision-makers
Source: A commissioned study conducted by Forrester Consulting on behalf of CyberGRX, May 2021

Key Recommendations ⟶



Key Recommendations

Forrester's in-depth survey about organizations' third-party cyber risk practices yielded several important recommendations:

Mature your third-party management program for reputational resilience.

Your third parties are an extension of your brand. When they fail, so do you. Your reputation depends on knowing and managing your third parties and building trust with your customers includes understanding your third-party risk. Review and assess — honestly and critically — whether your current practices for evaluating third-party risk properly serve your decision-making processes. Leveraging all available data (and automation practices to get the most from that data) ensures that your entire supply chain will meet your cyber requirements.

Require third parties to earn the right to do business with you.

A robust and detailed assessment of the third-party's cyber maturity is the first step — but not the last — in a strict onboarding process. Continual monitoring using threat intelligence and a remediation mindset is needed to protect the business and the customer. Be stringent and set a baseline for what you will and will not accept and enforce it in real time.

Training means everything: Create and nurture strong communication across all business units.

Communication among all parties is a critical piece of third-party cyber risk management. Your protection is only as strong as your weakest link. Break down existing siloed processes to ensure business stakeholders and IT/ risk management decision-makers are in tune with each other. These units operate independently and often make decisions without consulting each other, but a robust security strategy requires consistency and collaboration among these teams. Take this one step further and make security training for all employees and stakeholders mandatory. Constant communication regarding cyber posture and third-parties' compliance, and ongoing education for all involved is key to preventing threats.

Increase visibility through monitoring.

Monitoring the cyber risk of third parties can be the difference between life and death. Automating the evaluation process also frees up internal resources to focus on other value-added initiatives to further strengthen security and manage risk — a true win-win. Only work with the third-parties who meet your baseline criteria at a minimum through continual monitoring.

Appendix A: Methodology

In this study, Forrester conducted an online survey of 319 third-party cyber risk management decision-makers in IT/security roles at organizations in the US, the UK, France, Australia, and Germany to evaluate their organizations' security strategies, particularly concerning third-party risk. Respondents were offered a small incentive as a thank-you for their time spent on the survey. The study was completed in May 2021.

Appendix B: Demographics

GEOGRAPHY	
US	**51%**
UK	**17%**
France	**11%**
Australia	**11%**
Germany	**10%**

COMPANY SIZE	
$100 million to $499 million	**34%**
$500 million to $999 million	**26%**
$1 billion+	**41%**

THIRD-PARTY CYBER RISK MANAGEMENT STRATEGY RESPONSIBILITY	
Final decision-maker	**29%**
Part of a team making the decision	**40%**
Decision influencer	**30%**

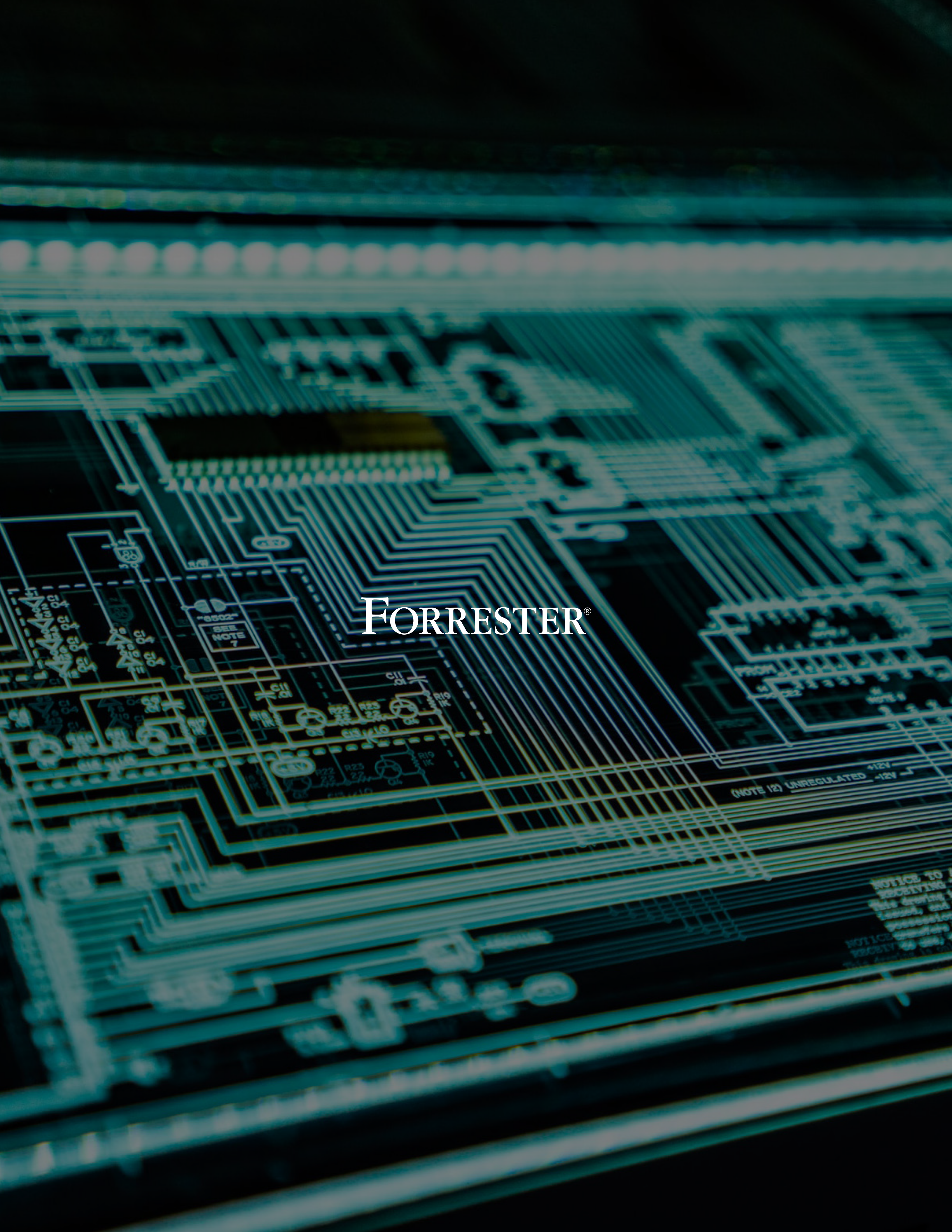
INDUSTRY	
Technology	**16%**
Retail	**16%**
Oil and gas	**16%**
Healthcare	**16%**
Financial services and insurance	**16%**
Other highly regulated industries	**21%**

LEVEL	
C-level	**8%**
VP	**17%**
Director	**30%**
Manager	**45%**

Appendix C: Endnotes

[1] Source: "Cost of a Data Breach Report 2021," Ponemon Institute, 2021.

Note: Percentages may not total 100 because of rounding.



FORRESTER®