



Enterprise Strategy Group | Getting to the bigger truth.™

RESEARCH HIGHLIGHTS

THE PRESSING NEED FOR COMPREHENSIVE CYBER RISK MANAGEMENT

Jon Oltsik, Senior Principal Analyst and ESG Fellow

DECEMBER 2019

CONTENTS

Research Objectives [3](#)

Key Research Findings [4](#)

Cyber risk management is increasingly important to both business executives and corporate directors. [5](#)

Executives and corporate boards are viewing more of their business through a risk management lens. [6](#)

Room for improvement between cyber and business risk team. [7](#)

Cyber risk management is more difficult today than in the past. [8](#)

Public cloud, software vulnerabilities, and increasingly sophisticated adversaries drive heightened cyber risk management complexity. [9](#)

Vulnerability management programs are plagued by abundant challenges that minimize their effectiveness. [10](#)

Organizations struggle with vulnerability lifecycle management. [11](#)

Organizations benefit from penetration testing and red teaming in multiple areas. [12](#)

The need for penetration testing tied to multiple organizational requirements. [13](#)

Cyber risk management best practices need to extend to strategic third parties. [14](#)

Reputation and experience are key considerations when it comes to third-party risk management. [15](#)

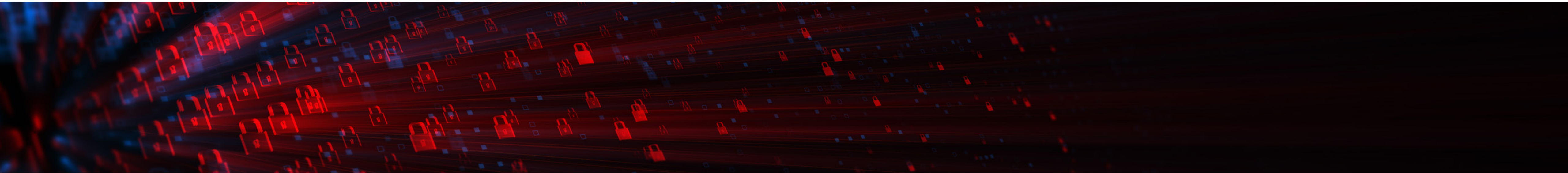
Many aspects of third-party security audits are still considered insufficient. [16](#)

Future risk management actions must align business and technology objectives. [17](#)

The vast majority of organizations expect to increase cyber risk management spending over the next 12 to 18 months. [18](#)

Research Methodology [19](#)

Respondent Demographics [19](#)



RESEARCH OBJECTIVES

Executives are increasingly reliant upon the availability of hybrid computing environments and distributed software applications for the smooth functioning of their organizations. As such, there is a growing requirement to be able to assess and mitigate cybersecurity risks associated with their IT environments.

In order to get more insight into these trends, ESG surveyed 340 IT and cybersecurity professionals at organizations in North America (U.S. and Canada) involved in planning, implementing, and/or enforcing IT risk management policies, processes, and strategies. This study sought to:

- Examine the state of cyber risk management today.
- Determine the most common cyber risk management weaknesses.
- Gain insight into how cyber risk management strategies and processes are evolving in order to better support business missions, initiatives, and operations.
- Understand how cyber risk management is impacting organizations' overall cybersecurity strategies.

Survey participants represented a wide range of industries including manufacturing, financial services, health care, communications and media, retail, government, and business services. For more details, please see the Research Methodology and Respondent Demographics sections of this report.

KEY RESEARCH FINDINGS

- 1. Cyber risk management is increasingly important to both business executives and corporate directors.** Business executives want real-time cyber risk information that can help them measure their cybersecurity status as it relates to major business/IT initiatives and IT and compliance audits.
- 2. Cyber risk management is more difficult today than in the past.** Attack surfaces continue to expand as organizations move to hybrid cloud architectures and add new devices to their networks. At the same time, there is a disconnect between business executives' need for real-time cyber risk management metrics and the technical data and periodic reports that cybersecurity teams are delivering.
- 3. Vulnerability management programs are plagued by abundant challenges that minimize their effectiveness.** Today's vulnerability management (VM) depends upon multiple tools, as well as massive data collection, processing, and analysis. VM processes and tools are complex, incomplete, and overwhelming. And despite VM investments, organizations still struggle to figure out which vulnerabilities to prioritize and which systems to patch.
- 4. Organizations benefit from penetration testing and red teaming in multiple areas.** These activities can identify hidden vulnerabilities and risks that can help IT and executive management prioritize risk mitigation actions. While penetration testing and red teaming produce numerous benefits, organizations continue to conduct these exercises on a periodic basis.
- 5. Cyber risk management best practices need to extend to strategic third parties.** Vendors, partners, SaaS platforms, suppliers, customer systems, and others may all be linked to an organization's IT systems. Organizations need visibility into these connections, but today's third-party risk management processes are based upon point-in-time assessments rather than continuous monitoring.
- 6. Future risk management actions must align business and technology objectives.** Security leadership (CISOs/CSOs) needs to be prepared to provide increasing amounts of risk visibility to business leaders and board members. This may be accomplished through a combination of additional communications, continuous monitoring, formal metrics, and more expansive cybersecurity risk management programs.

Cyber risk management is increasingly important to both business executives and corporate directors.



Executives and corporate boards are viewing more of their business through a risk management lens.

Executive managers and corporate boards are increasingly pushing CISOs and other senior cybersecurity leaders to focus on cyber risks as they relate to organizational objectives. This includes detecting, prioritizing, monitoring, and reporting on cyber risk metrics in a manner that is consumable by non-technical business leaders.

When asked to identify the cyber risk metrics they believe are most important to the business executives and corporate directors in their organizations, 39% of respondents identified security status reports related to major business and IT initiatives. In other words, non-IT leaders want to understand cyber risk at a high level as it relates to end-to-end business processes, so cybersecurity teams need to do a better job translating security data into business metrics. Other key metrics include compliance audit results (36%), overall environment vulnerability assessments (36%), and ROI for cybersecurity spending (35%).

» Top 4 cyber risk metrics for business executives and corporate directors



39%
Security status related to major business/IT initiatives



36%
Status and response associated with IT and compliance audits



36%
Reports related to the risk of the vulnerabilities in my environment, correlated with other security data



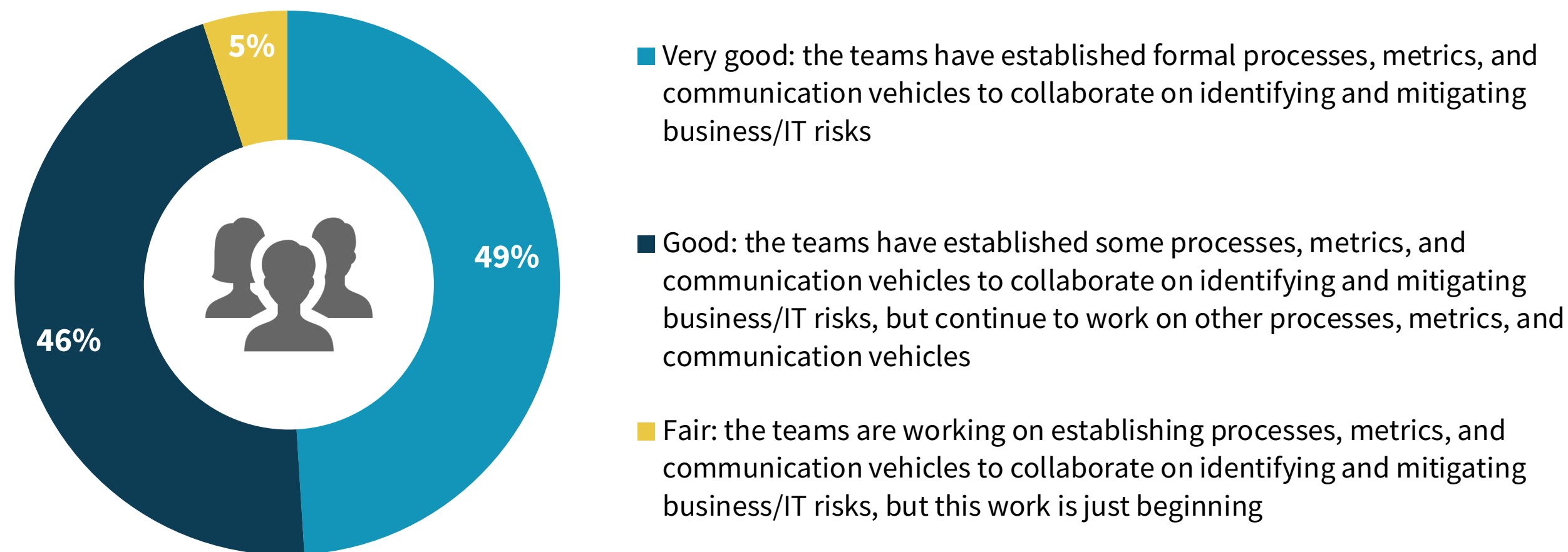
35%
ROI on cybersecurity spending

Room for improvement between cyber and business risk team.

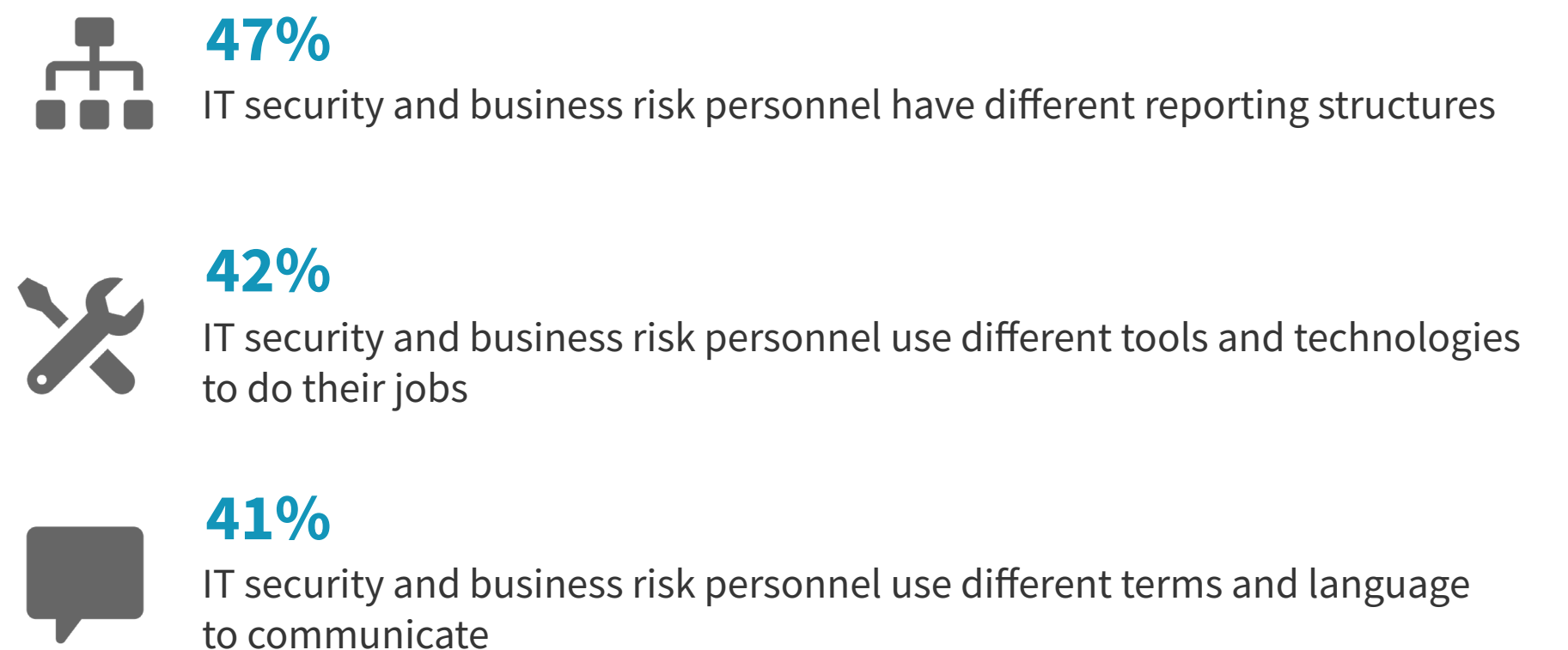
Cyber risk management can be extremely difficult, as CISOs rely on a plethora of disconnected systems and processes to discover assets, track system and application vulnerabilities, monitor threats, and understand data flows. Additionally, many CISOs have few (if any) systems of record that aggregate risk data and provide the capabilities to report cyber risk in a business context.


When asked to describe how cyber risk and business risk teams work together, most respondents indicated there is room for improvement. Specifically, while nearly half (49%) labeled the relationship as very good, the majority acknowledged there is work still to be done—in some cases, a substantial amount—to refine the processes, metrics, and communication vehicles for collaboration between the two groups.

» Cyber risk and business risk relationships



In terms of the challenges to establishing and maintaining a strong relationship between cyber and business risk teams, nearly half (47%) pointed to the disparate reporting structures of the two groups. The other commonly cited challenges included the use of different tools and technologies (42%) and terms and language to communicate (41%).



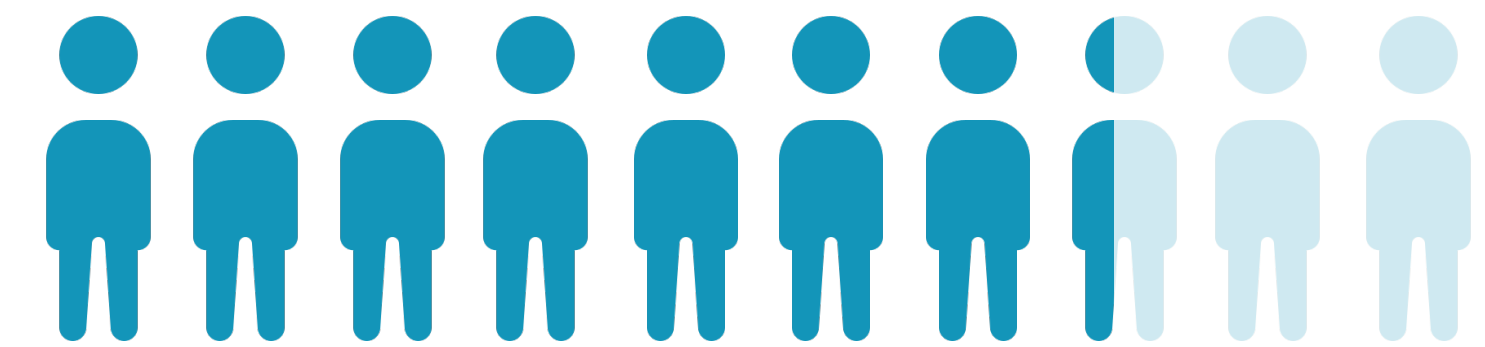


**Cyber risk management
is more difficult today
than in the past.**

Public cloud, software vulnerabilities, and increasingly sophisticated adversaries drive heightened cyber risk management complexity.

Organizations increasingly operate in an ever expanding, digitally interconnected, and dangerous world. At the same time, the attack surface continues to expand, as workloads and data are increasingly shifting to the cloud as new devices are deployed on corporate networks. These trends are creating a range of internal and external cyber risk management challenges. When asked about their organizations' technologies, policies, and processes related to cyber risk management activities, nearly three-quarters (73%) of respondents said these tasks have become more difficult over the last two years.

Among those respondents indicating increased difficulty handling cyber risk management, the plurality of respondents identified more workloads being deployed on public cloud infrastructure services (43%). While more technically sophisticated adversaries was also cited, the common thread among the other top drivers of heightened cyber risk complexity is volume, including more software vulnerabilities (42%), sensitive data (41%), and devices on the network (39%).



73%
say risk management is more difficult

» Top 5 reasons why cyber risk management has become more difficult


43%
My organization has moved more workloads to public cloud infrastructure services

42%
Number of software vulnerabilities has increased

42%
Technical sophistication of adversaries has increased

41%
My organization has more sensitive data

39%
There are more devices connected to our network

A man with dark hair and glasses is shown in profile, looking intently at a computer screen. The background is dark, with various data visualizations and code snippets overlaid on the image, suggesting a technical or cybersecurity environment. The text is prominently displayed on the left side of the image.

**Vulnerability
management programs
are plagued by abundant
challenges that minimize
their effectiveness.**

Organizations struggle with vulnerability lifecycle management.

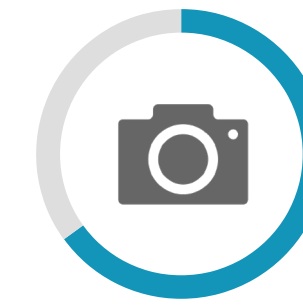
Organizations are increasingly exposed due to the overwhelming volume of software vulnerabilities, the sheer amount of network-resident sensitive data that is unaccounted for, and the lack of real-time visibility and monitoring capabilities.



70%
believe the volume of software vulnerabilities is overwhelming



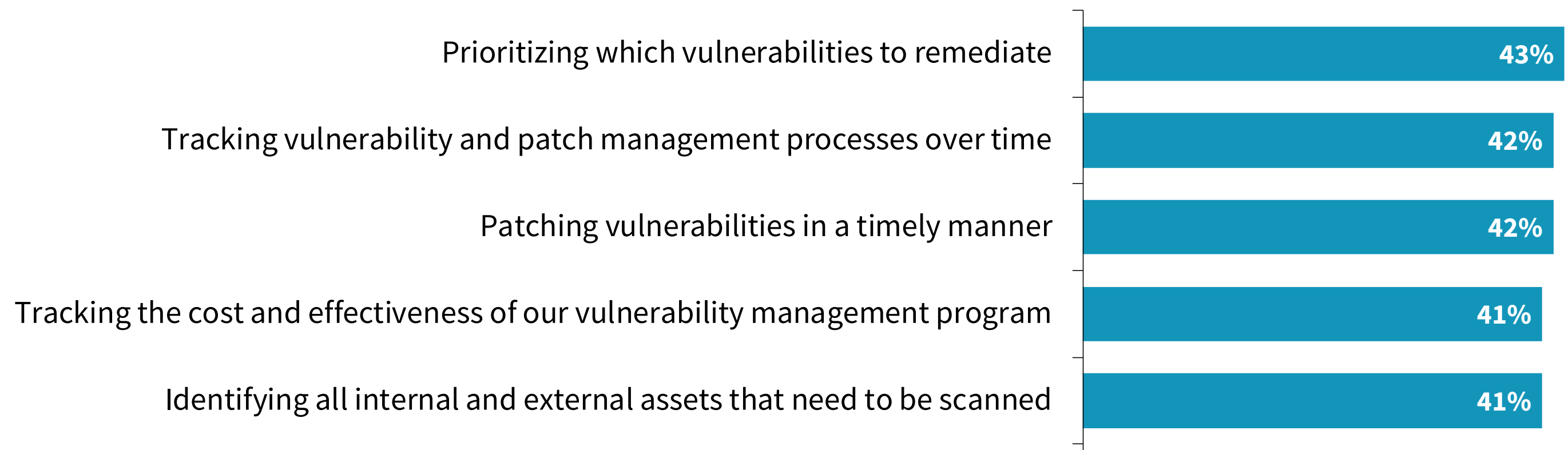
68%
believe they have unaccounted for sensitive data on their network




65%
believe risk management is too dependent on point-in-time assessments

Given that nearly three-quarters of respondents believe that software vulnerability levels are overwhelming, it follows that prioritizing (43%) and patching (42%) these vulnerabilities are the most commonly cited vulnerability management challenges. Tracking these efforts over time is also proving difficult for organizations, whether it's specific patch management processes or the cost and effectiveness of an overall vulnerability management program. There is a clear and present need for technologies and processes that help organizations track, quantify, prioritize, measure, and communicate the risks associated with widespread vulnerabilities in a way that is universally understood and that can be acted upon.

» Top 5 vulnerability management challenges



An aerial photograph of a city, likely Los Angeles, with a dense grid of buildings and streets. Overlaid on the image are numerous colorful, glowing lines in shades of red, orange, yellow, green, and blue, representing data flow or network connections. The lines are most prominent in the foreground and middle ground, creating a sense of dynamic movement and connectivity. The sky is filled with soft, white clouds, and the overall lighting is bright and clear.

**Organizations benefit
from penetration testing
and red teaming in
multiple areas.**

The need for penetration testing tied to multiple organizational requirements.

Most large organizations do some type of penetration testing or red teaming exercises annually. When asked about the primary reason driving these efforts, more than half identified one of the following: they are a best practice for risk assessment (26%), they are a regulatory compliance requirement (17%), or they are a mandate from executive management and/or the board of directors (14%). Typical penetration testing/red teaming projects last two weeks and few organizations have the resources and skills to do these activities on their own.

» Penetration Testing Rationale



Length of typical penetration testing/red teaming projects:



TWO WEEKS

Penetration testing and red teaming produce results. Half of organizations leverage penetration testing results to measure the responsiveness of IT and security teams when it comes to identifying and remediating vulnerabilities. Other common uses involve reviewing report findings with leadership teams for both IT (49%) and line of business (46%), as well as utilizing the results to determine what security and IT processes could be reinforced (45%) and where security and IT teams could benefit from additional training (40%). Clearly, penetration testing and red teaming can be extremely useful tools for cyber risk management. Therefore, CISOs must explore ways to perform these exercises on a continual basis.



50%

Measures security and IT teams on their ability to address and remediate vulnerabilities in a timely fashion



49%

Reviews all reports with IT leaders



46%

Reviews all reports with non-technical leaders



45%

Uses reports to reassess security and IT processes

Cyber risk management best practices need to extend to strategic third parties.



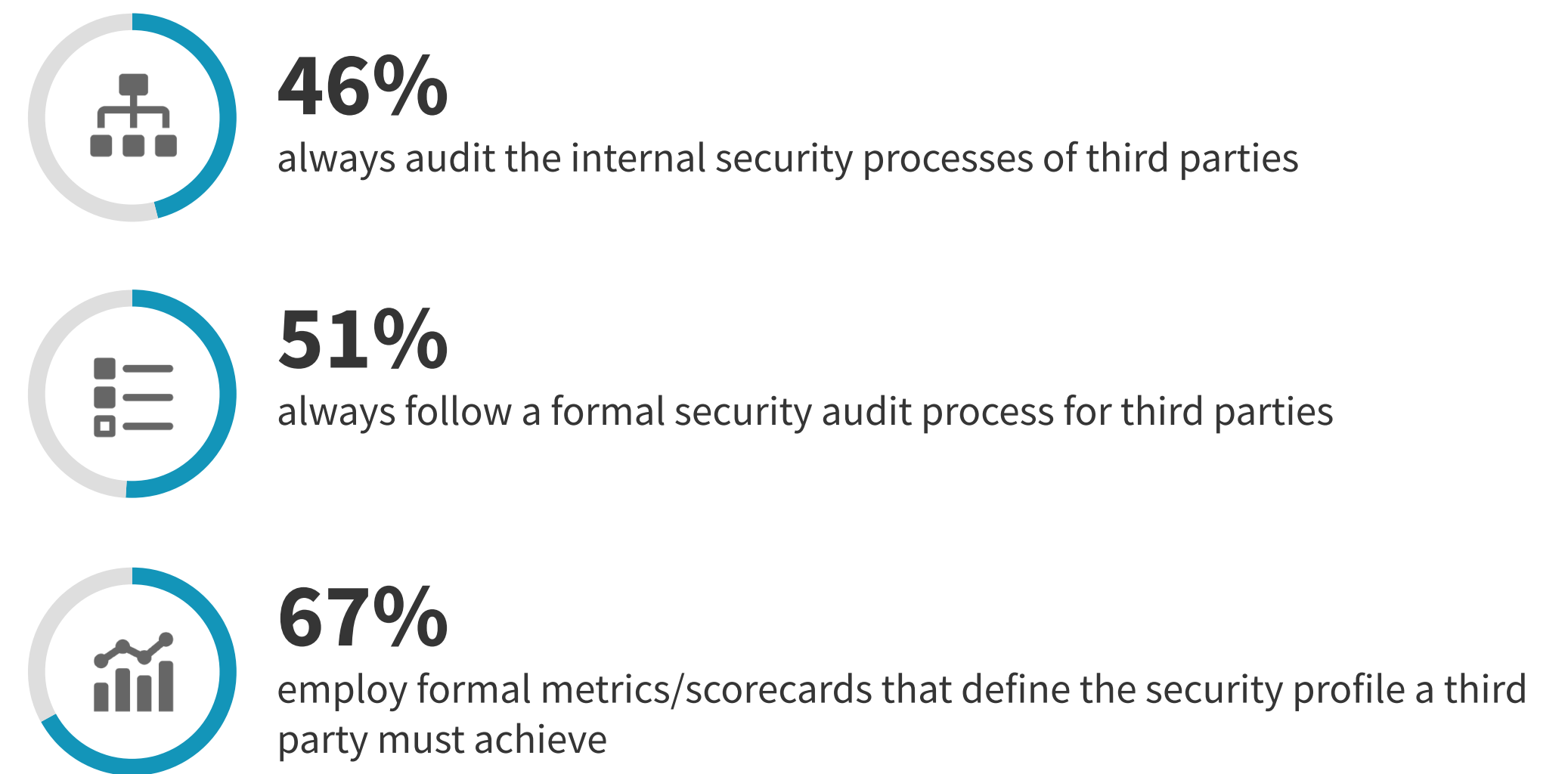
Reputation and experience are key considerations when it comes to third-party risk management.

How do organizations' risk management strategies account for interactions with third parties? Cybersecurity and risk managers tend to look at historical and static data to establish a cyber risk baseline for each third-party organization. Specifically, reputation plays a significant role in terms of evaluation or consideration criteria, whether at a specific security expertise level (35%) or at a more general industry experience level (28%). One-third factor in security breaches previously experienced by third parties, while 27% of organizations consider ISO certifications and/or emergency response procedures.

» Top 5 third-party risk management criteria



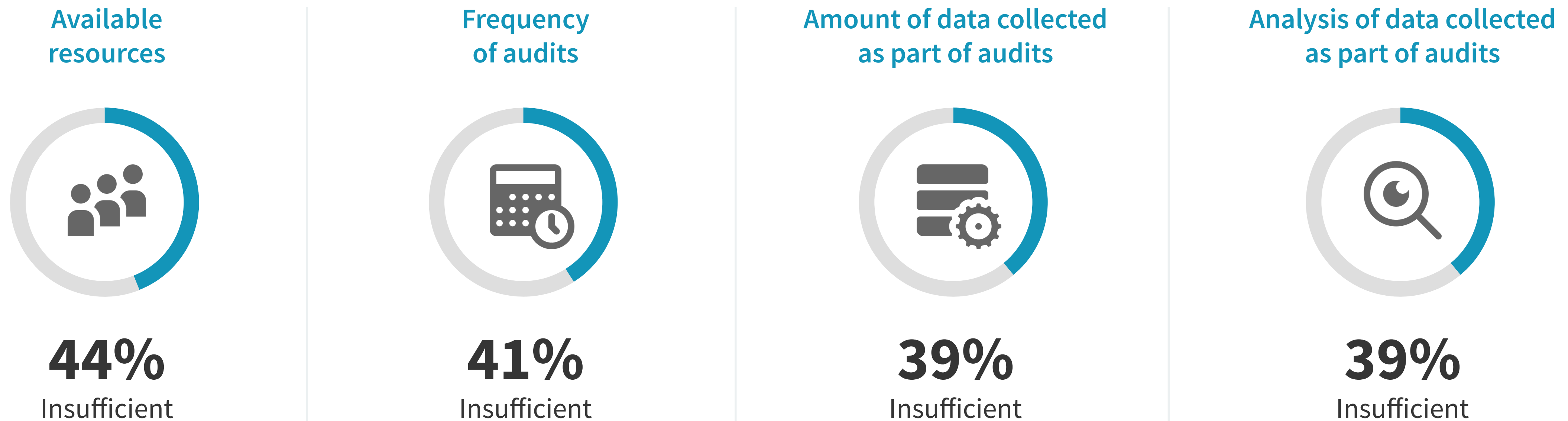
Best practices for risk management dictate that organizations always audit the internal security processes of third parties, employ a formal security audit process that must be followed in all cases, and employ formal metrics/scorecards that third parties must achieve before organizations will work with them. Yet, only slightly more than one-quarter (28%) of respondent organizations employed **all three** of these best practices.



Many aspects of third-party security audits are still considered insufficient.

Effective third-party risk management may require the ongoing assessment of dozens or even hundreds of outside organizations. However, many organizations—in some cases, more than four in ten—don't believe they have enough available resources for the job, audit frequently enough, collect enough data as part of these audits, and/or perform enough analysis on the data collected. Therefore, it may be helpful to work with service providers who can provide continuous monitoring, alerting, and advanced analytics for third-party risk.

» Insufficient aspects of third-party security audit processes



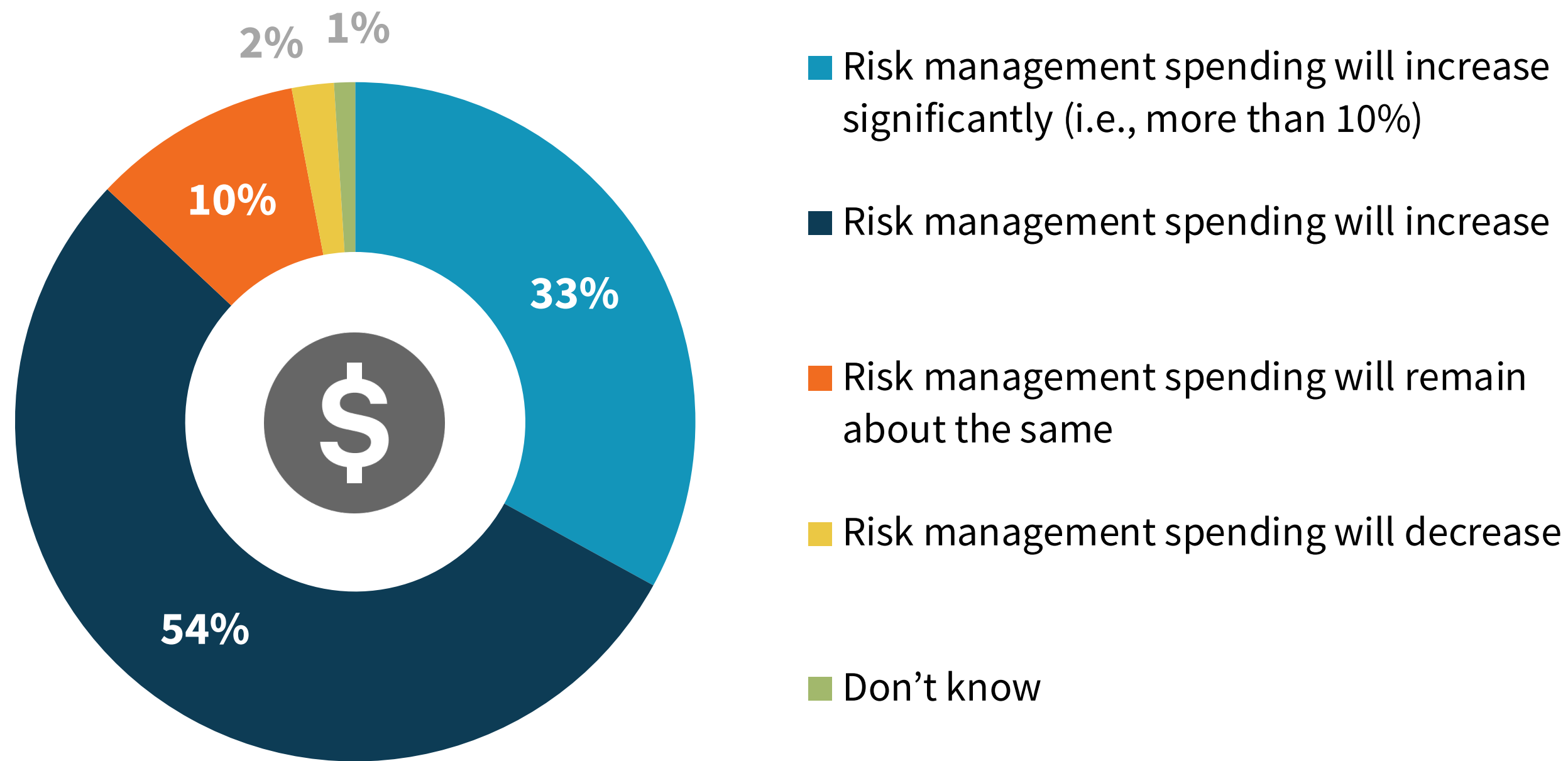
Future risk management actions must align business and technology objectives.



The vast majority of organizations expect to increase cyber risk management spending over the next 12 to 18 months.

There is a gap between the need for the right data, analysis, and metrics, and the ability of the GRC teams to provide them. Security leadership (CISOs/CSOs) must be prepared to provide increasing amounts of visibility to their business leaders and board members. This may be accomplished through a combination of additional communications, continuous monitoring, defined metrics, and more expansive cybersecurity risk management programs. To bridge the cyber risk management gap, 87% of organizations plan on increasing cyber risk management spending over the next 12-18 months, with one-third anticipating this increase to be significant.

» Cyber risk spending change over the next 12 to 18 months



» Top 4 actions to improve cyber risk management



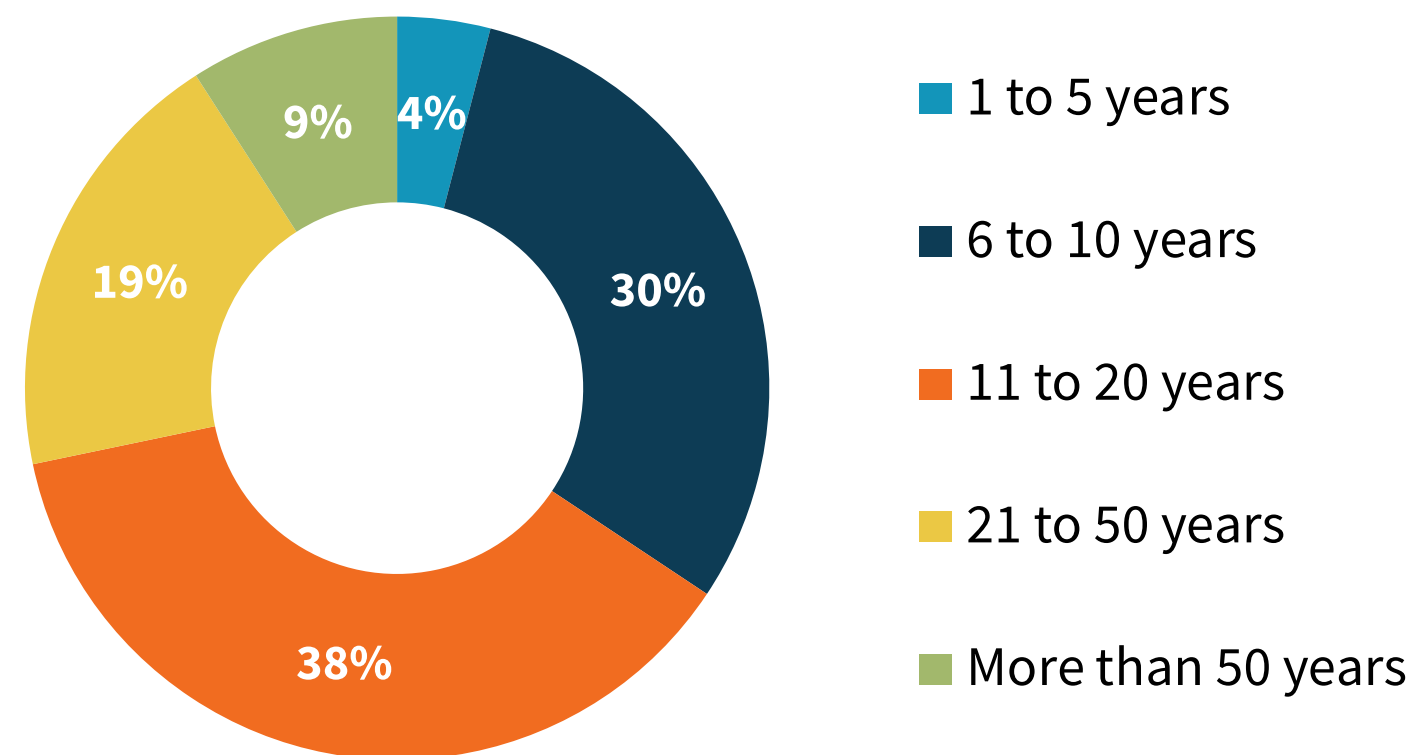
Research Methodology

To gather data for this report, ESG conducted a comprehensive online survey of IT and cybersecurity professionals from private- and public-sector organizations in North America (United States and Canada) between October 3, 2018 and October 24, 2018. To qualify for this survey, respondents were required to be IT or cybersecurity professionals involved in planning, implementing, and/or enforcing IT risk management policies, processes, and strategies. All respondents were provided an incentive to complete the survey in the form of cash awards and/or cash equivalents.

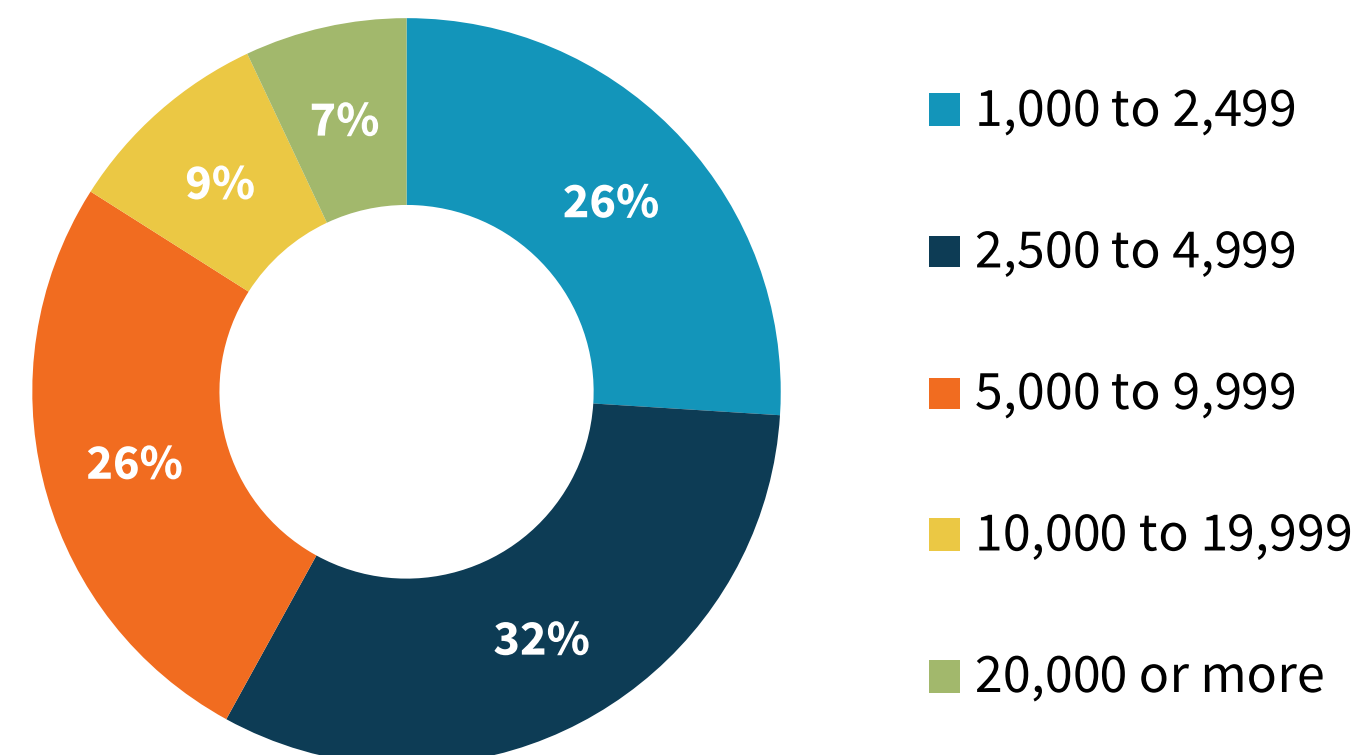
After filtering out unqualified respondents, removing duplicate responses, and screening the remaining completed responses (on a number of criteria) for data integrity, we were left with a final total sample of 340 IT and cybersecurity professionals.

Respondent Demographics

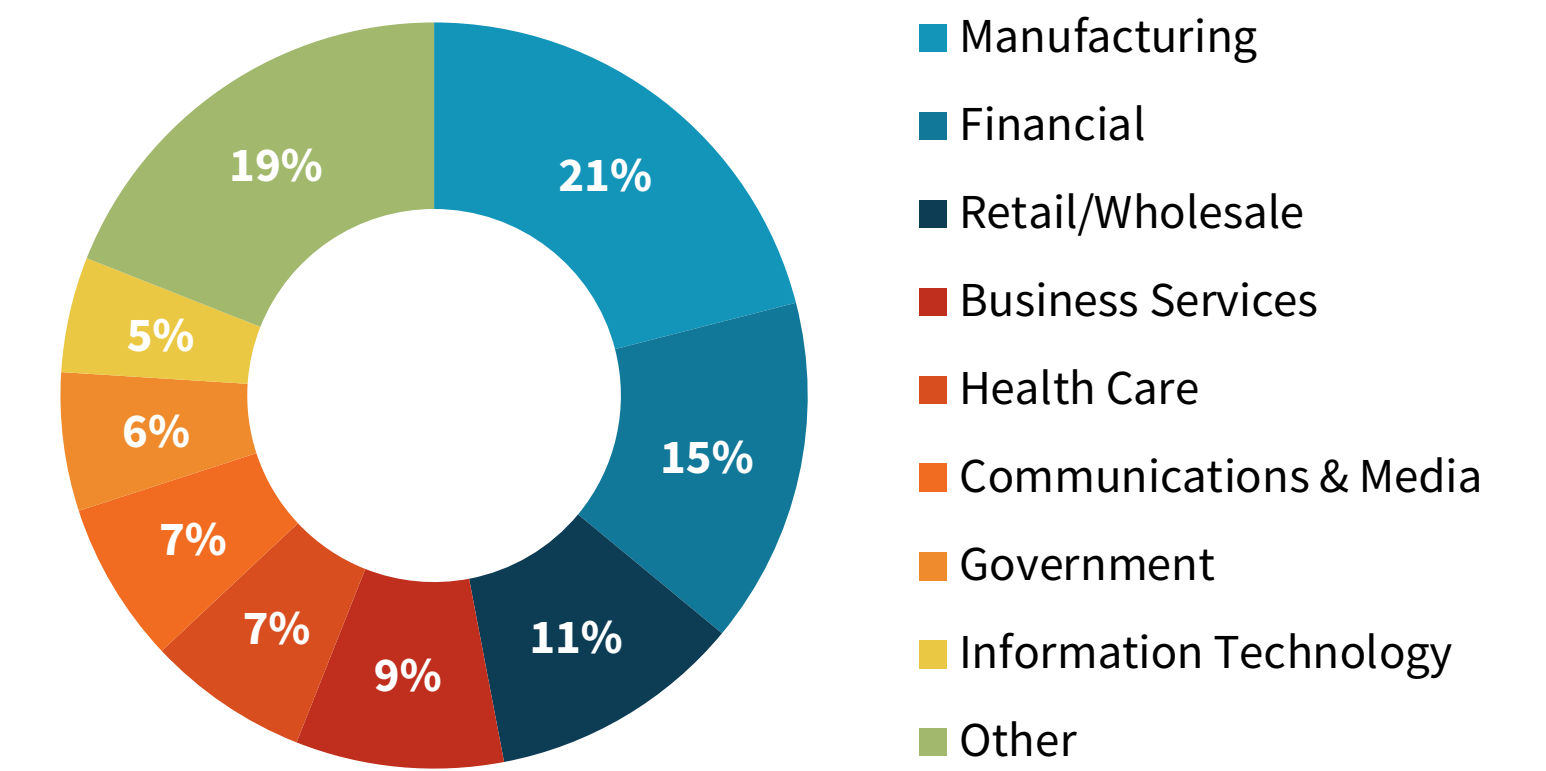
Respondents by Age of Organization



Respondents by Number of Employees Worldwide



Respondents by Industry





ServiceNow (NYSE: NOW) is making the world of work, work better for people.

Our cloud based platform and solutions deliver digital experiences that create great experiences and unlock productivity for employees and the enterprise.

[LEARN MORE](#)

ABOUT ESG

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.



All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change from time to time. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of The Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at 508.482.0188.



Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides actionable insight and intelligence to the global IT community.
© 2019 by The Enterprise Strategy Group, Inc. All Rights Reserved.