



Enterprise Strategy Group | Getting to the bigger truth.™

RESEARCH HIGHLIGHTS

Cybersecurity in the C-suite and Boardroom

Jon Oltsik, Senior Principal ESG Analyst, ESG Fellow

JANUARY 2021





CONTENTS

Research Objectives	3
Research Highlights	4
Cybersecurity is still largely perceived as a technology area.	6
Cyber-risk management is increasing.	9
Corporate boards are getting more engaged with cybersecurity but still have a long way to go.	12
Enterprise cybersecurity programs remain uneven.	15
Organizational cybersecurity gaps remain.	17
There is plenty of room for improvement.	21
Recommendations	23

Research Objectives

As organizations embrace digital transformation initiatives, business outcomes become inexorably linked to technology areas like application development, cloud computing, and IoT devices. Therefore, these technology assets must be protected to ensure continuity of business operations. The link between cybersecurity and the business has led to an industry declaration that, “Cybersecurity is a boardroom issue.” This statement is true yet simplistic. Executives and corporate directors have a fiduciary responsibility to shareholders and/or owners, so they are ultimately responsible for everything that drives the business, including managing cyber-risk and safeguarding business-critical technology assets. That said, cybersecurity can be a highly technical discipline. This brings up a few questions: Do executives really understand cybersecurity and its role in the business? And as technology further dominates the business landscape, are they investing appropriately in cybersecurity and driving a cybersecurity culture throughout their organizations?

To explore the answers to these and other questions, ESG surveyed 100 senior business, cybersecurity, and IT professionals at organizations in Western Europe (UK, France, and Germany) working at midmarket (i.e., 100 to 999 employees) and enterprise-class (i.e., more than 1,000 employees) organizations.

THIS STUDY SOUGHT TO:



Explore the role of cybersecurity in the business.



Uncover where progress is being made and areas that need more focus and investment.



Examine the relationships between security and business executives.



Compare the actions of leading organizations with those that lag behind.

Research Highlights

CYBERSECURITY IS STILL LARGELY PERCEIVED AS A TECHNOLOGY AREA.

Most business and technology leaders believe that cybersecurity is entirely or mostly a technology area with little or no linkage to the business. Additionally, many organizations rate themselves as only adequate or poor in areas like their executives' commitment to cybersecurity and treating cybersecurity as a critical component of business strategies. In aggregate, the research indicates that most organizations don't strive for "good security," but rather they settle on "good enough" security.

CYBER-RISK MANAGEMENT IS INCREASING.

To manage risk, organizations piece together aspects of a multiple of frameworks, models, and services such as the NIST cybersecurity framework, ISO 31000, and the Factor Analysis of Information Risk (FAIR). Despite these guidelines, however, 77% of European organizations claim that cyber-risk has increased over the past 2 years due to factors like increasing cyber-threats, greater executive and board of director cybersecurity involvement, and more compliance requirements.

CORPORATE BOARDS ARE GETTING MORE ENGAGED WITH CYBERSECURITY BUT STILL HAVE A LONG WAY TO GO.

Many board members are more active with cybersecurity education, leading to a situation where 82% of corporate boards are more engaged in cybersecurity than they were two years ago. Still, many boards must be drawn into cybersecurity through some type of catalyst, like new regulatory compliance requirements, the introduction of a new cybersecurity program, or in reaction to a data breach in the organization's industry.





ENTERPRISE CYBERSECURITY PROGRAMS REMAIN UNEVEN.

When senior business, cybersecurity, and IT managers stack ranked aspects of their organization's cybersecurity program, engineering and SDLC, endpoint security, and third-party risk management were the most immature areas. Organizations are investing in program areas like IT operations, cloud security, and information security. In other words, they don't seem to be intent on improving the immature areas of their programs.

ORGANIZATIONAL CYBERSECURITY GAPS REMAIN.

Despite CISOs and CIOs typically having a close relationship, nearly half of respondents claim that the relationship between security and IT teams is only somewhat well aligned or not very well aligned. While security and IT do relatively well in collaborating on security technology deployment and IT infrastructure, they aren't nearly as well coordinated in areas like application security, DevOps, or end-user support. Other corporate executives are often only somewhat involved or not very involved in other areas of cybersecurity like establishing a cybersecurity culture or prioritizing security investments.

THERE IS PLENTY OF ROOM FOR IMPROVEMENT.

Respondents had plenty of suggestions for improving the alignment of cybersecurity and the business like bringing the security team into business planning, increasing cybersecurity training for board members and executives, and improving data analysis for decision support.

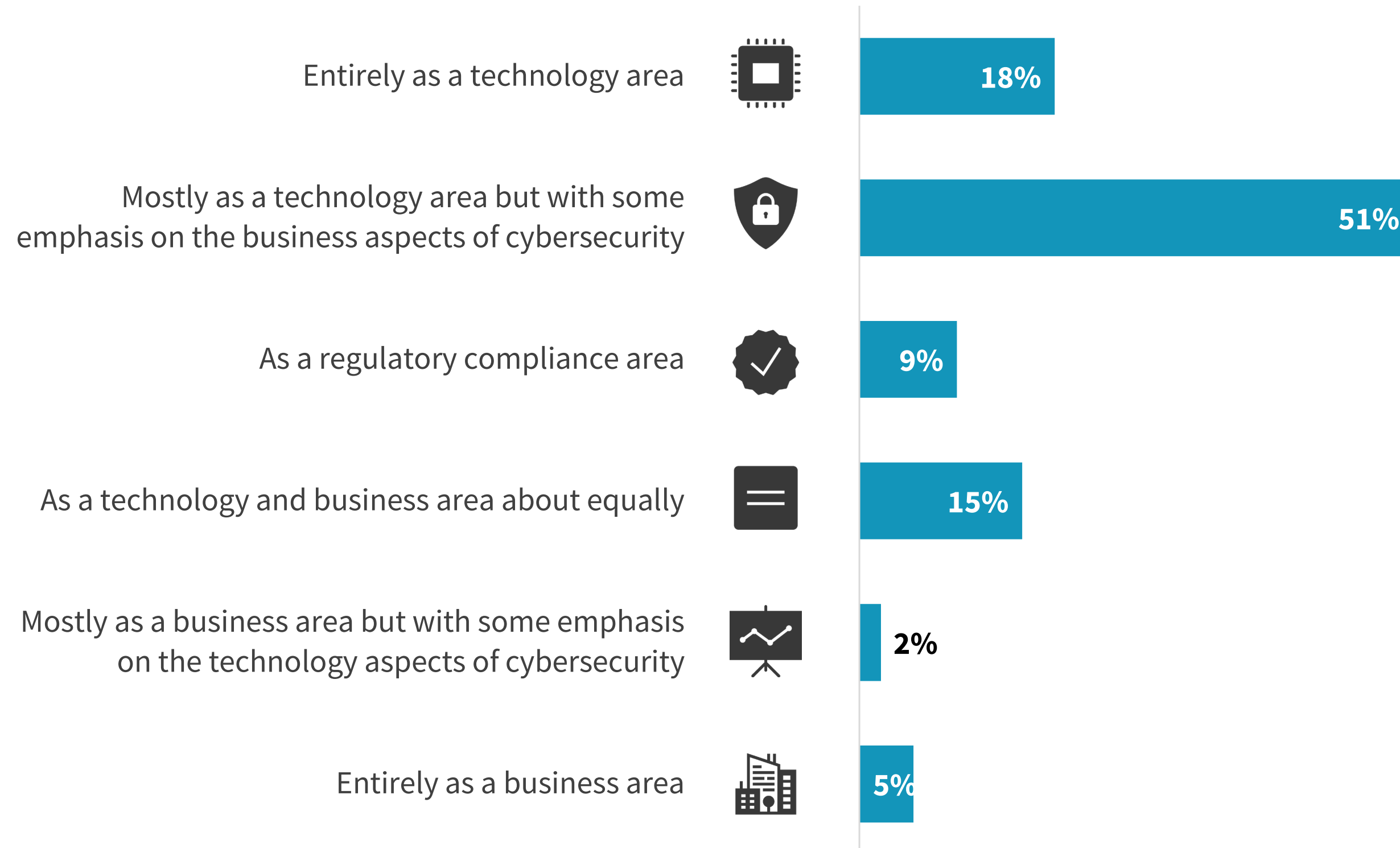
Cybersecurity is still largely perceived as a technology area.

Cybersecurity Still Viewed as a Technology Area, but There Is Progress

Nearly three-quarters (73%) of European respondents view cybersecurity as part of the business mission, at least to some extent, compared to only 58% of their North American counterparts. Perhaps more noteworthy is the fact that European organizations are significantly less likely to view cybersecurity as entirely a technology area (versus 32% of organizations in North America). This is likely due to Europe's progressive commitment to data privacy through GDPR, forcing closer cybersecurity and business collaboration.

“ Nearly three-quarters (73%) of European respondents view cybersecurity as part of the business mission, at least to some extent, compared to only 58% of their North American counterparts.”

How cybersecurity is viewed.

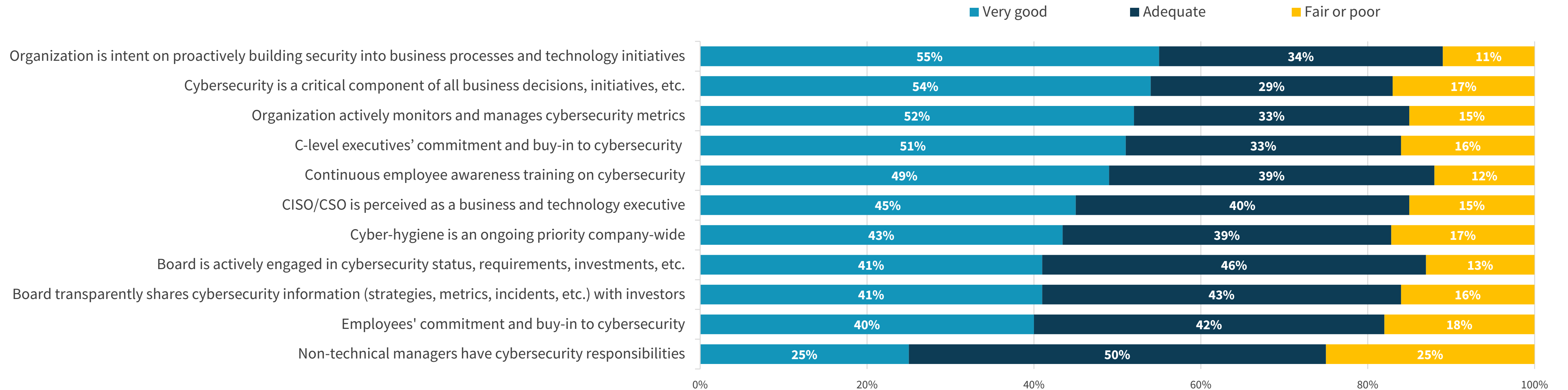


A Large Percentage of Organizations Remain Content with ‘Good Enough Security’

Cybersecurity professionals often lament that their organizations don’t want good security; they want “good enough” security. In other words, business executives are only willing to fund cybersecurity people, processes, and technologies that help the organization comply with regulations and provide basic protection. Unfortunately, ESG’s data indicates that this minimalist attitude remains persistent in several areas. For example, less than half of European respondents rate their C-level executives’ commitment to cybersecurity (49%) or their organization’s intention to build cybersecurity into business processes and IT initiatives (45%) as only adequate or fair, and 56% rate their company-wide commitment to cyber-hygiene as adequate, fair, or poor.

Clearly, many organizations are minimizing their commitment to cybersecurity. This increases cyber-risk and makes the application of cybersecurity controls complex and costly. CISOs should assess their organizations in each of these 11 areas to help them decide which cybersecurity initiatives should be prioritized in the next board meeting.

Cybersecurity organizational culture.



A person's hands are seen typing on a keyboard in a dimly lit room. In the background, several computer monitors are visible, displaying various data and charts. The overall atmosphere is blue and tech-oriented.

**Cyber-risk management
is increasing.**

Organizations Rely on Multiple Risk Management Standards, Leading to Varied Metrics and Complex Operations

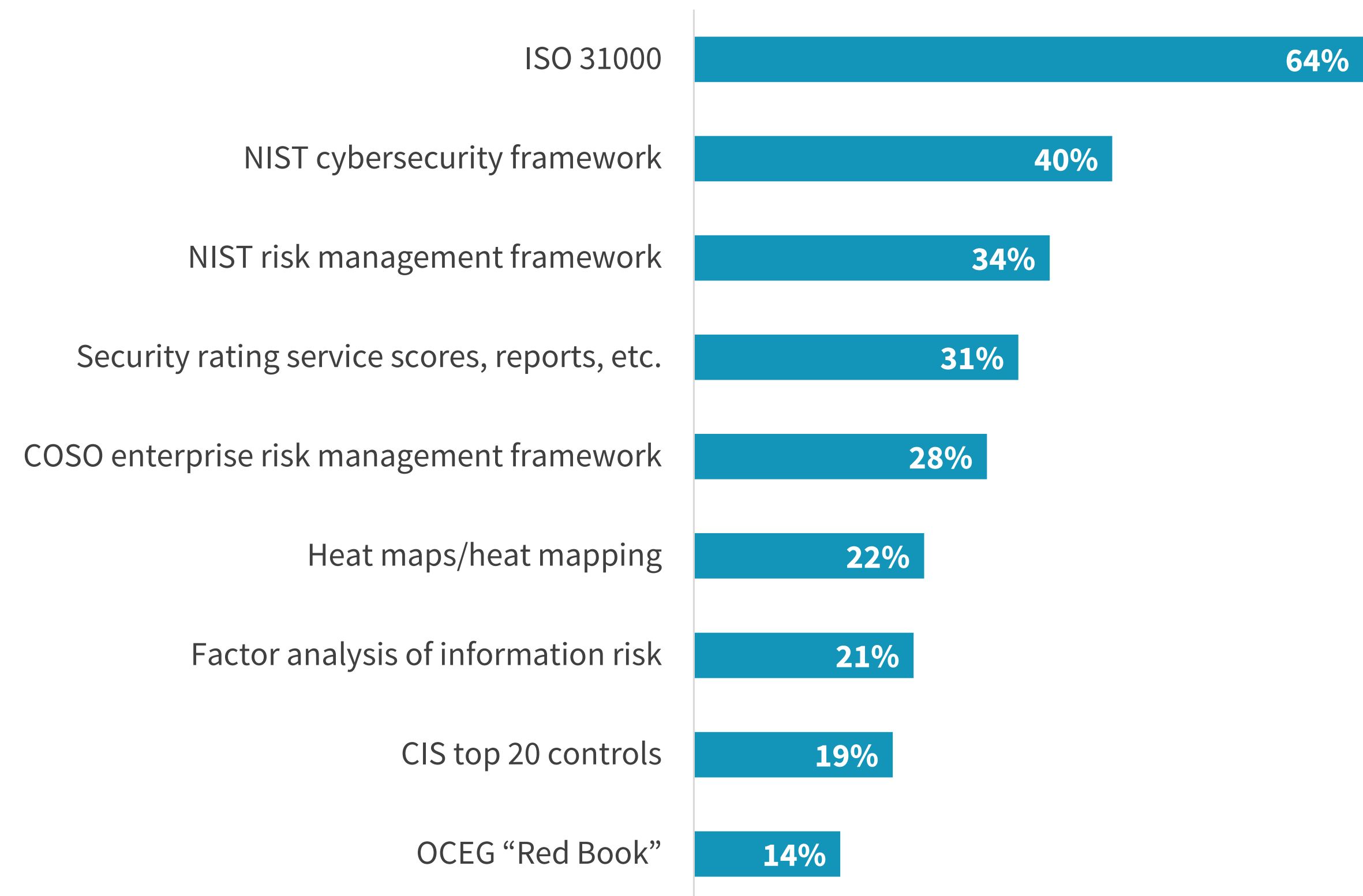
Ask any CISO to identify their primary responsibility and they'll likely tell you it is managing and mitigating cyber-risks to the business. To accomplish this task, nearly two-thirds of European organizations utilize ISO 31000 to benchmark, measure, and control cyber-risk. Additionally, these organizations employ numerous frameworks, standards, or security scorecards and rating services.

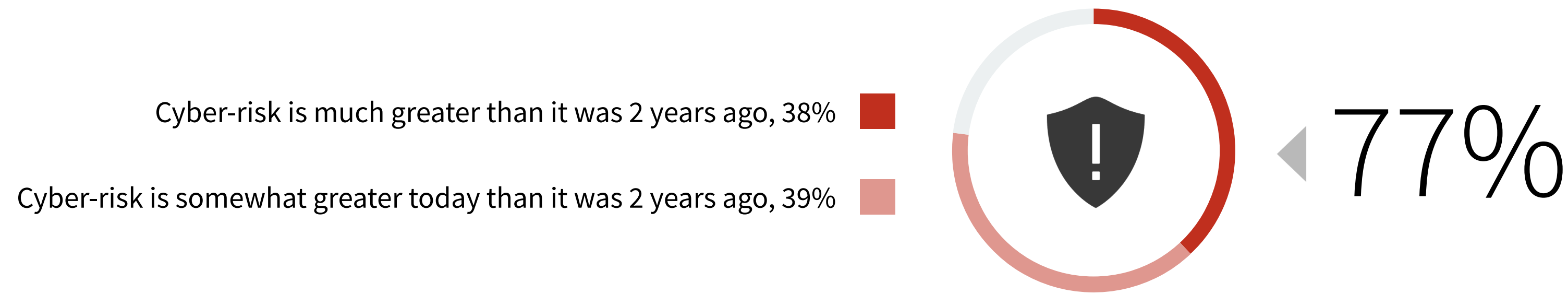
CISOs tend to create their own risk management guidelines by piecing together industry standard frameworks deemed as the best fit for their organizations. While this can help them categorize and manage cyber-risk, it also creates a customized risk management framework, making it more difficult to input external data or compare internal and external risk factors. Each CISO seems to have their own preferred cyber-risk management model, so each time an organization changes its security executive, it begins anew with cyber-risk management and an associated enterprise cybersecurity program.

CISOs should network with other industry security executives in pursuit of a more universal cyber-risk management standard. This would help them compare results and share best practices with other similar organizations.

“ CISOs tend to create their own risk management guidelines by piecing together industry standard frameworks deemed as the best fit for their organizations.”

Frameworks and standards used to benchmark cyber-risk.





Drivers of heightened cyber-risk levels.



Cyber-risk Is Increasing Due to External Factors and Business Practices

A vast majority of European organizations (77%) believe that cyber-risk has increased over the past two years. What's behind this increase? While more than half of these respondents point to an increase in cyber-threats, greater executive/board participation in cybersecurity (31%) and an increase in regulations (30%) were also cited.

As cyber-risks rise, it's important to make sure that business and IT initiatives are supported by the right level of security oversight and controls. Why? Digital transformation initiatives are often built on new technologies like microservices, utilize IoT devices, change rapidly, and collect and process large data repositories, introducing new security vulnerabilities. Given this situation, a targeted attack could lead to business disruption or a costly data breach. Mitigating these risks depends upon strong cooperation between business, IT, and security teams from the initial planning stages of digital transformation projects.

Corporate boards are getting more engaged with cybersecurity but still have a long way to go.

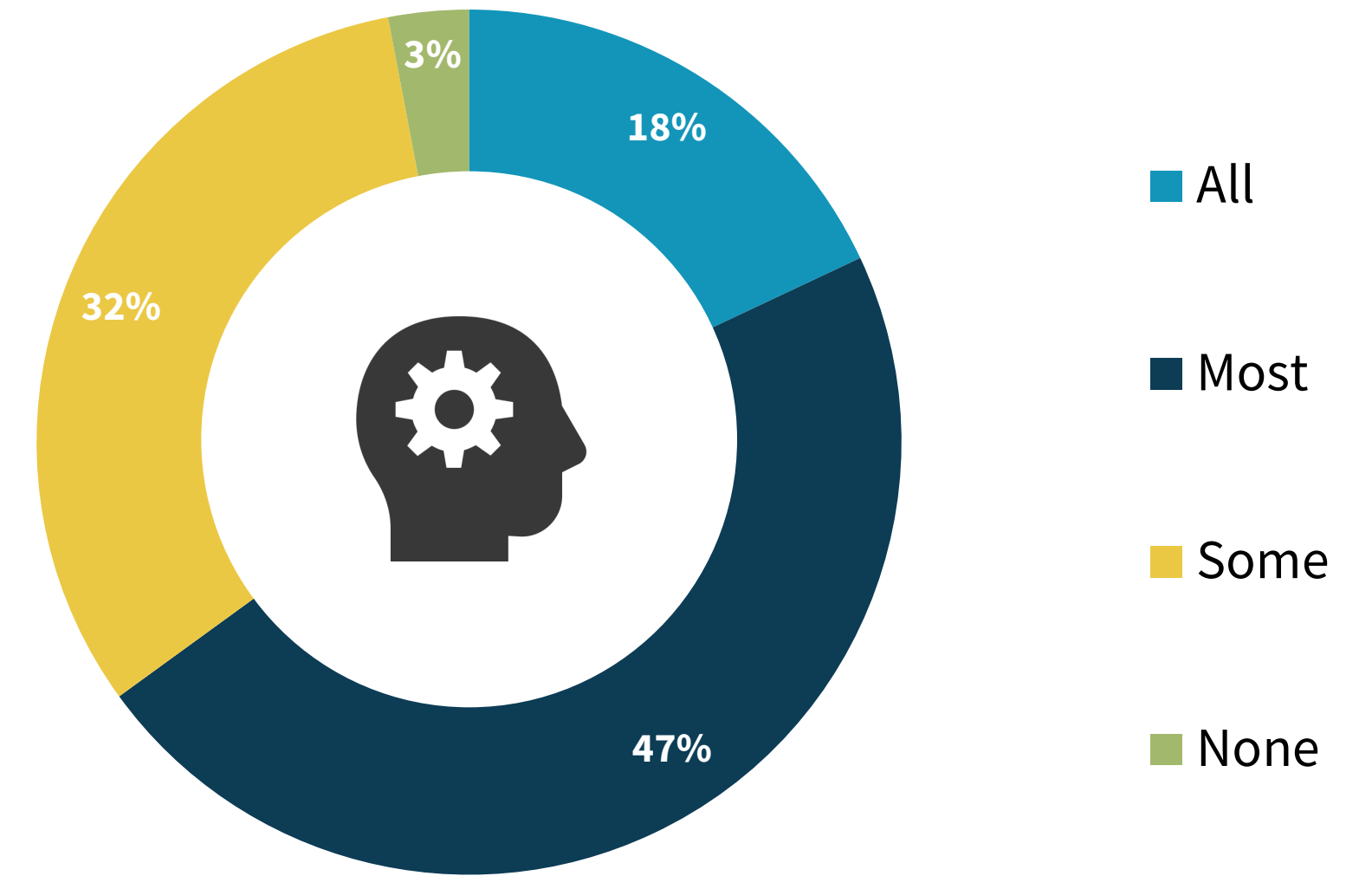


Four in Ten European Corporate Boards Engage in Continuous Cybersecurity Education

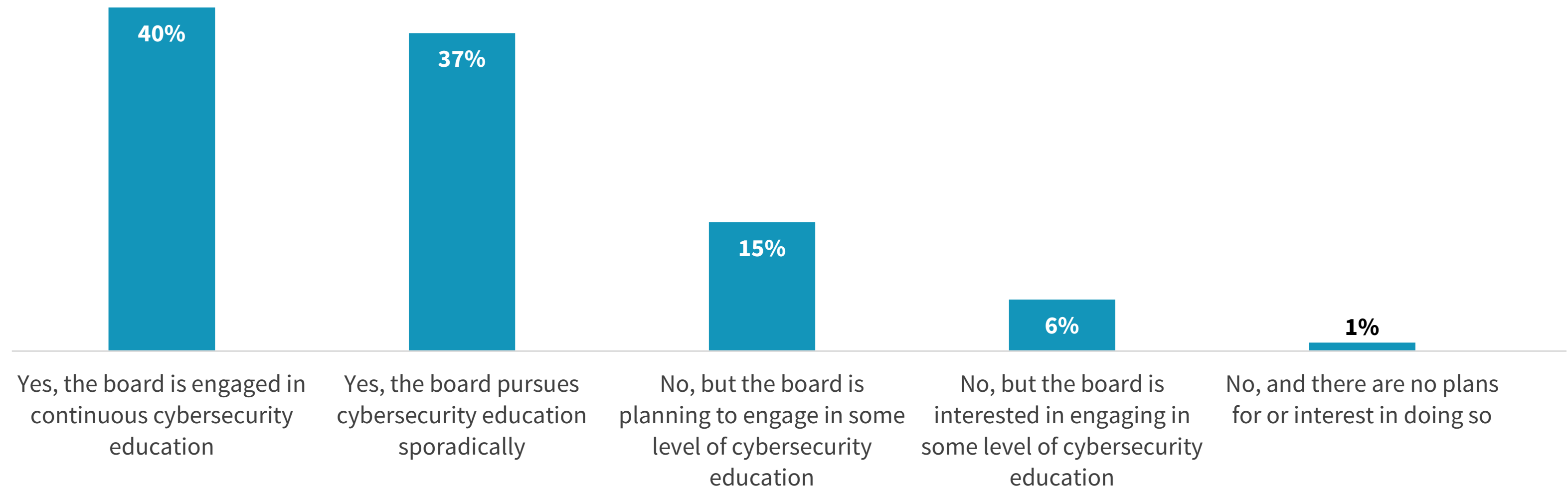
While nearly 80% of European organizations indicate that most (47%) or at least some (32%) of their board members are knowledgeable about cybersecurity, only 18% placed all of their members in this category. Not surprisingly, just 40% of European organizations say that their board of directors engages in some type of continuous cybersecurity education, noticeably lower than North America counterparts (53%). Usually, this is the CISO's responsibility, but some organizations bring in outsiders for board-level cybersecurity education. ESG believes this is a best practice that should be pursued more broadly.

Board members knowledgeable about cybersecurity.

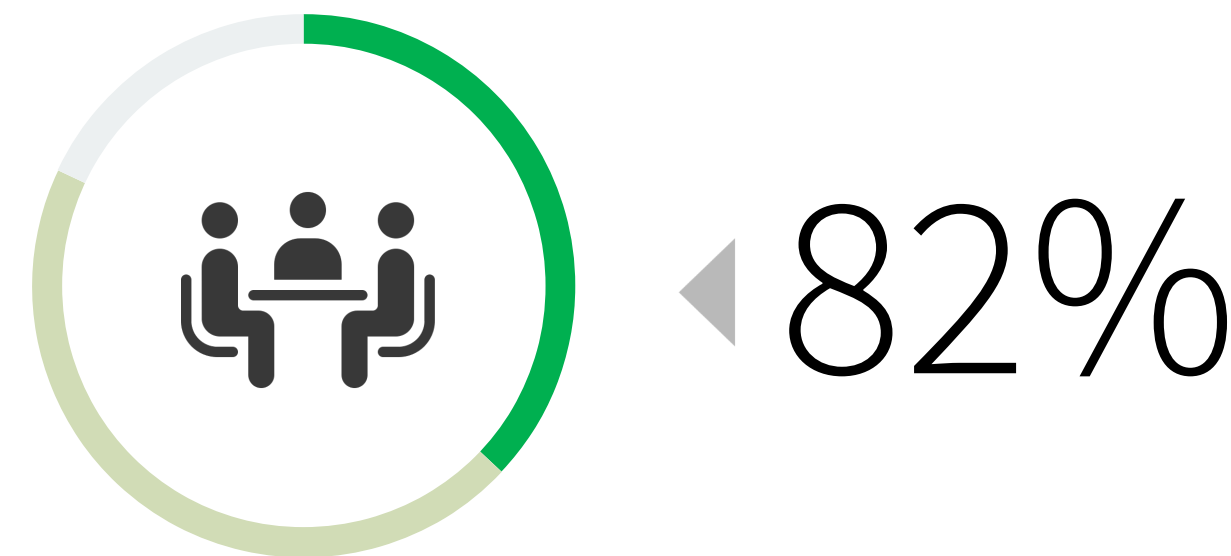
“ 40% of European organizations say that their board of directors engages in some type of continuous cybersecurity education.”



Board of directors' level of engagement with cyber education.



- The board of directors is **much more** engaged with cybersecurity status, decisions, and strategy than it was 2 years ago, 37% ■
- The board of directors is **somewhat more** engaged with cybersecurity status, decisions, and strategy than it was 2 years ago, 45% ■

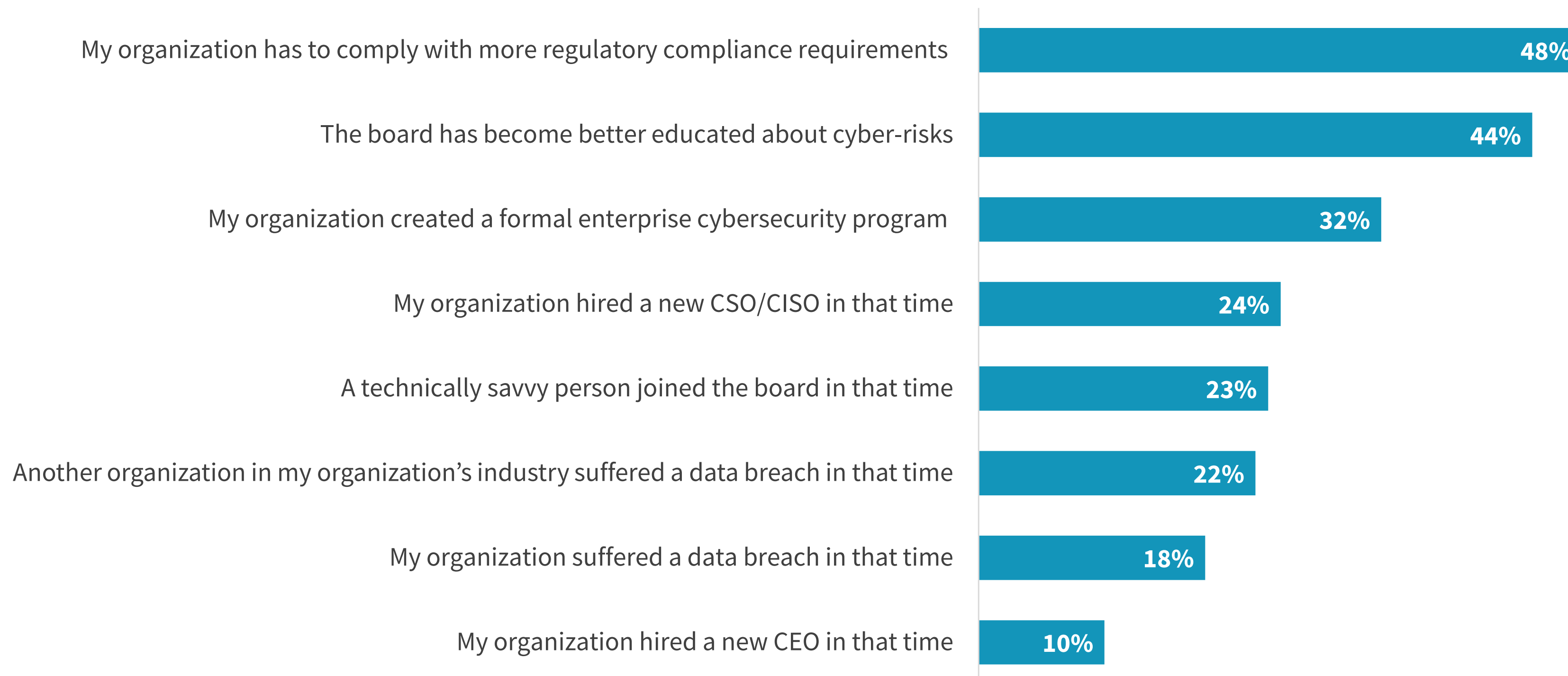


Corporate Boards Have Become More Engaged with Cybersecurity

A majority (82%) of European organizations say that their board is more engaged with cybersecurity today than it was two years ago for several reasons. New regulatory compliance requirements are forcing boards to become more involved with cybersecurity. Alternatively, board members have become more educated on cybersecurity than in the past. When board members are more educated, they ask tougher questions, dig into issues, and make the leap from cybersecurity to business issues. Finally, boards become more engaged with the introduction of a cybersecurity program (by the CISO).

Rather than wait to be drawn in, corporate boards at leading organizations are driving this agenda on their own.

Reasons for more cyber-engaged boards of directors.



**Enterprise
cybersecurity
programs remain
uneven.**

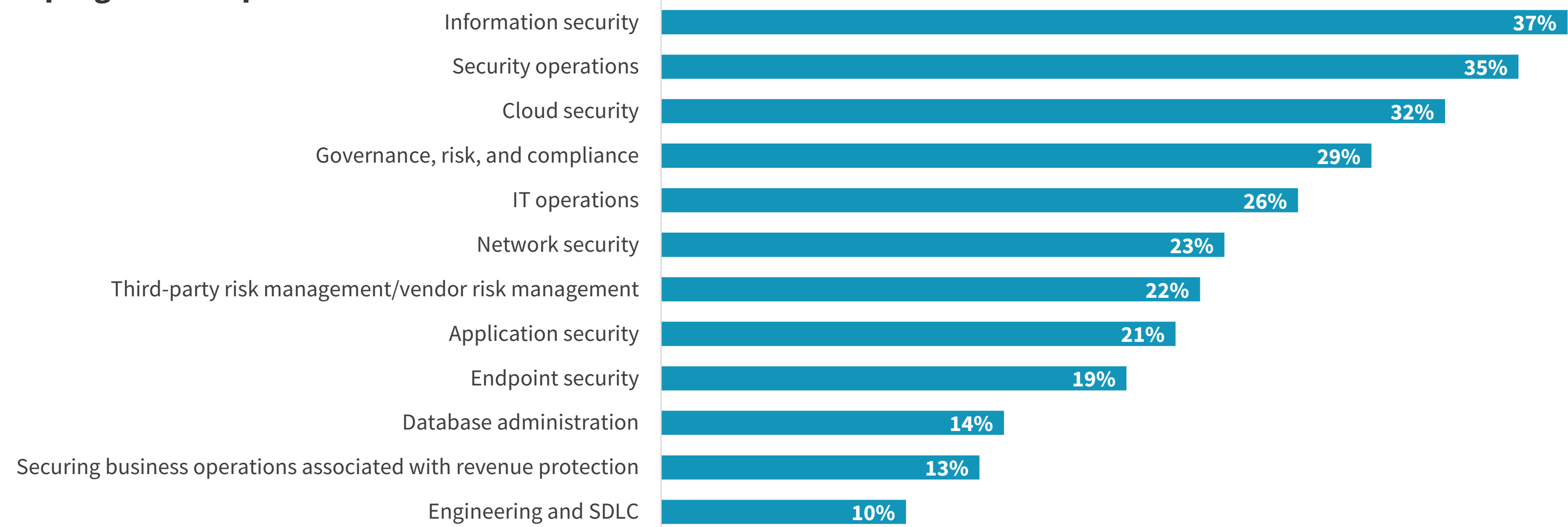


Maturity Levels of Cybersecurity Program Areas Vary, as Do the Subsequent Investment Levels

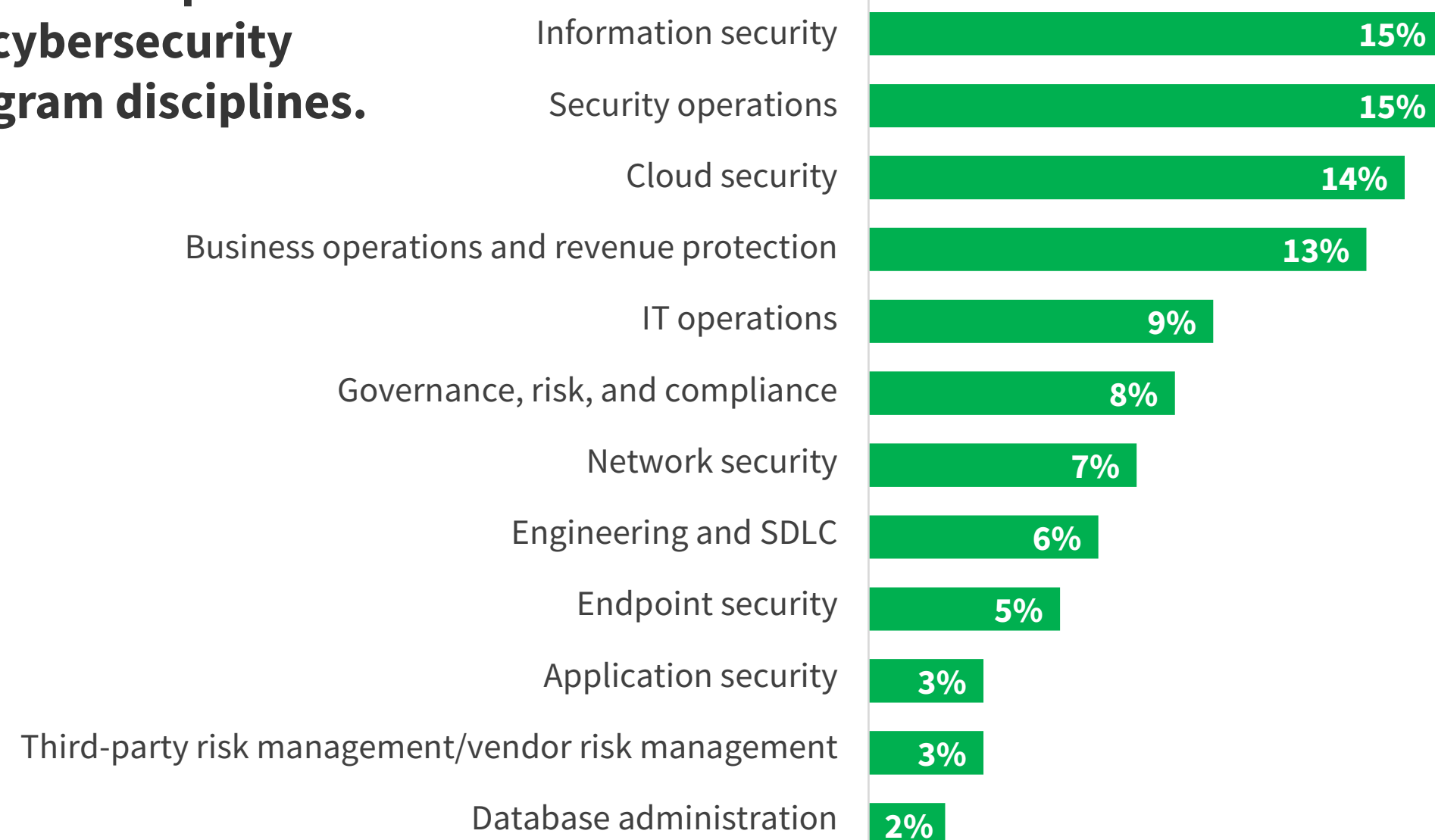
An enterprise cybersecurity program should include multiple areas with focus and investment skewed to areas that support business operations. When asked which program areas are most mature, 37% of European respondents identified information security (i.e., protecting the confidentiality, integrity, and availability of sensitive data), 35% said security operations (i.e., threat prevention, detection, and response, etc.), and 32% pointed to cloud security (i.e., security of cloud-based applications, data, and workloads). It's worth noting that European organizations are more mature than their North American counterparts in areas like GRC (29% versus 15%) and third-party risk management (22% versus 13%).

In terms of investments, European organizations prioritize security operations, information security, cloud security, and business operations. It is disappointing, however, that European organizations are not investing more in areas like application security, security engineering/SDLC, or endpoint security as these disciplines have been profoundly impacted by the acceleration of digital transformation and work-from-home (WFH) initiatives driven by the global pandemic.

Most mature cybersecurity program disciplines.



Investment priorities for cybersecurity program disciplines.



**Organizational
cybersecurity
gaps remain.**

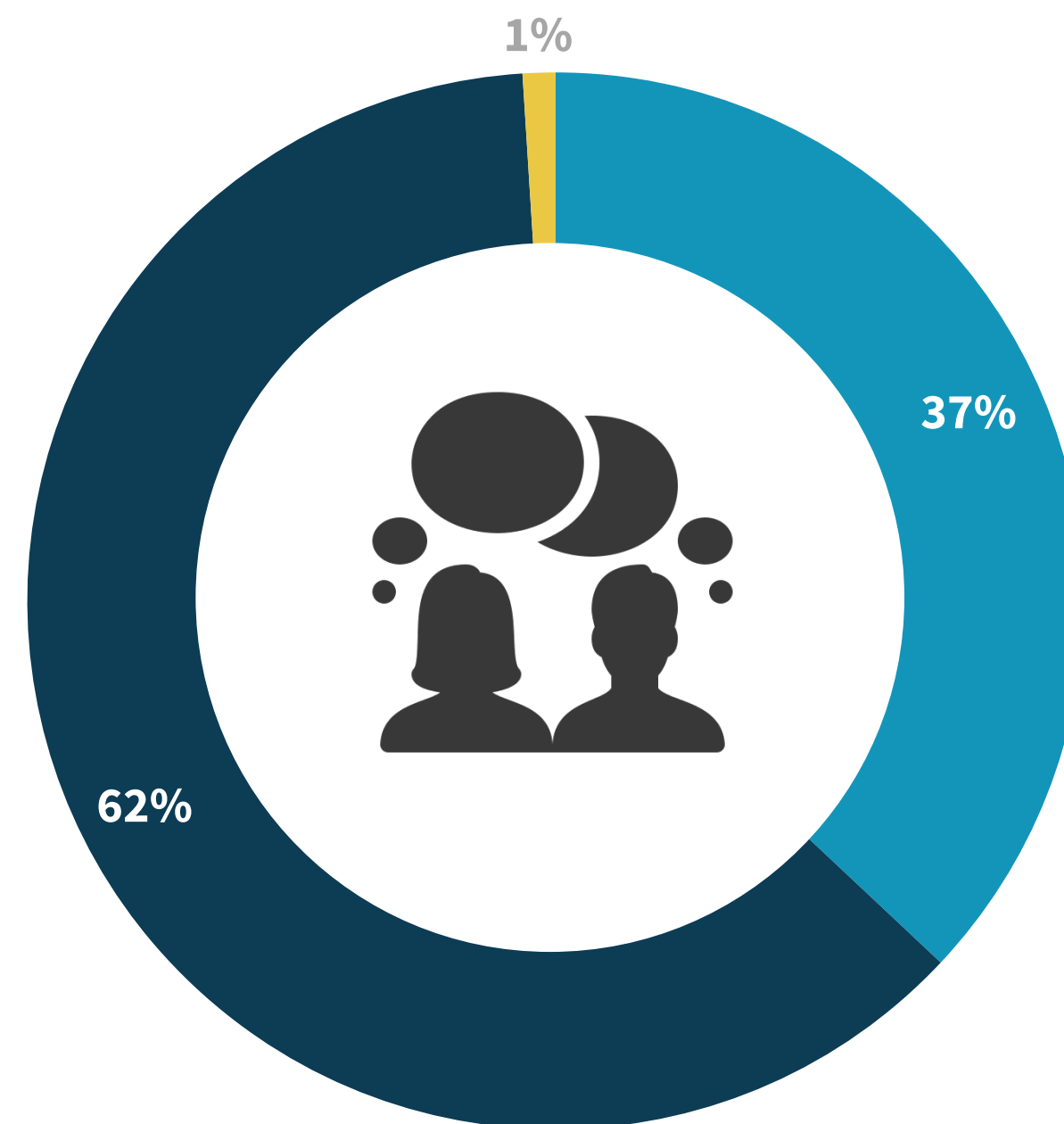


Security and IT Teams Are Not Well-aligned at Most Organizations

While the research indicates that CISOs work more closely with CIOs than any other executives, security and IT teams don't always do as well. Nearly two-thirds (62%) of European respondents say security and IT teams are only somewhat well-aligned, meaning security is sometimes, but not always, part of IT planning and implementation. This lack of alignment is especially concerning, as these two groups must collaborate in areas that could impact the business like protecting critical IT assets, monitoring activities, and mitigating risk.

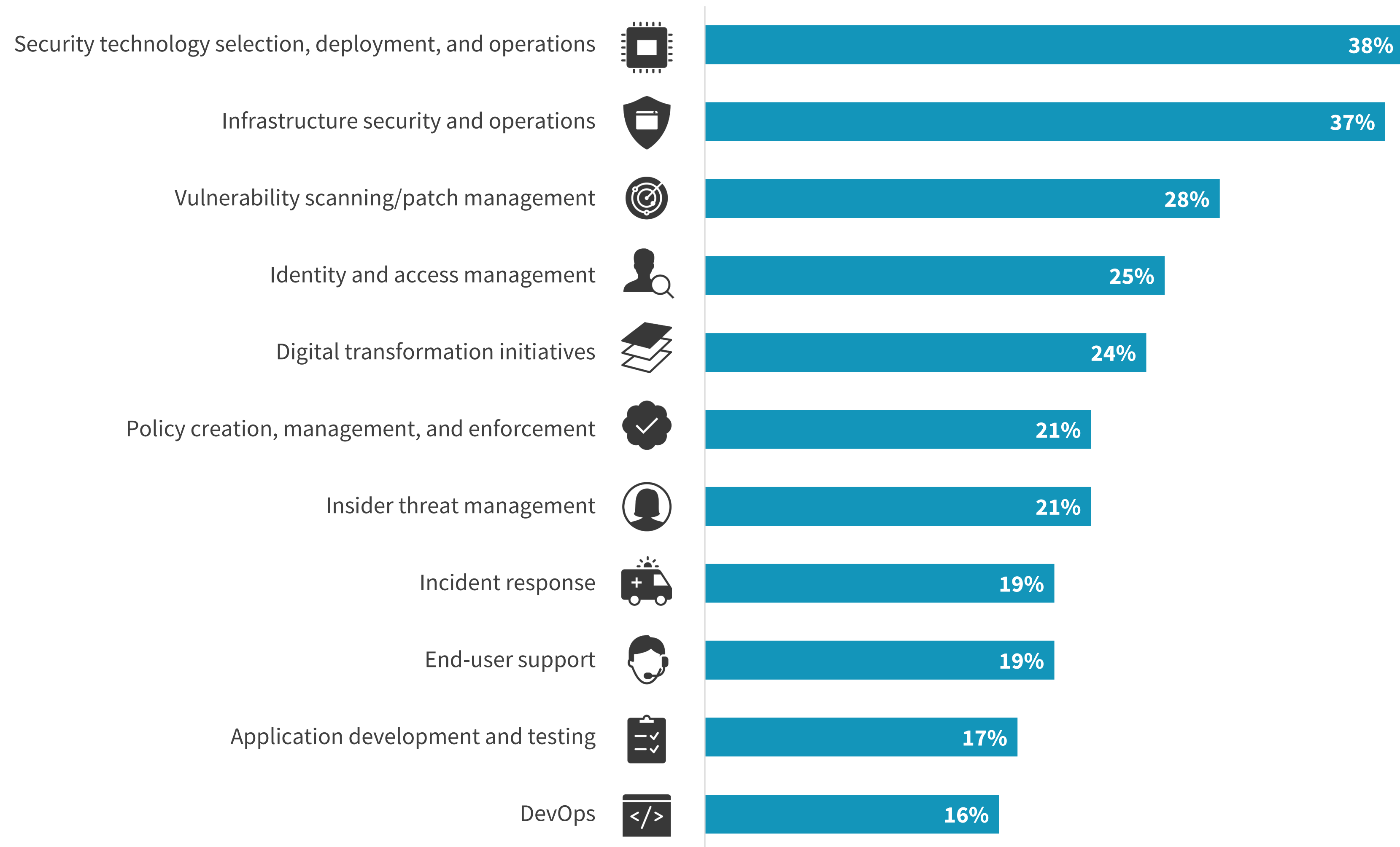
“ Nearly two-thirds (62%) of European respondents say security and IT teams are only somewhat well-aligned.”

| Alignment between IT and cybersecurity groups.



- Very well-aligned: security is part of IT project planning, implementation, and operations
- Somewhat well-aligned: security is sometimes, but not always part of IT project planning, implementation, and operations
- Not well-aligned: security is rarely part of IT project planning, implementation, and operations

Areas of greatest synergy between IT and cybersecurity groups.



IT and Cybersecurity Cooperation Is Skewed Toward Fundamental Areas

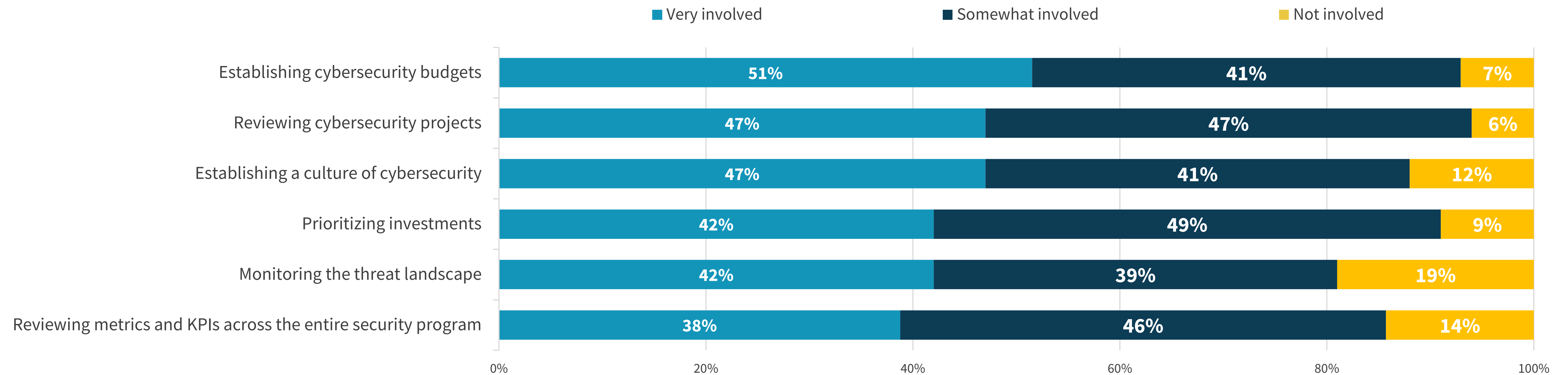
ESG’s research also reveals that security and IT groups work best together in areas like security technology selection, deployment, and operations; and infrastructure security and operations. This isn’t surprising as security and IT teams have been doing things like configuring servers, deploying firewalls, and inspecting network traffic for over 20 years. What is concerning, however, is that European security and IT teams aren’t nearly as coordinated with other requirements like DevOps, end-user support, and application development/testing. Furthermore, only 24% of respondents say that IT and security teams work best on digital transformation initiatives. This is somewhat alarming as digital transformation initiatives drive modern businesses, so security and IT teams should be tightly coordinating activities from the onset of all projects.

Executives Remain Cursory to Cybersecurity Activities

When it comes to executive involvement in cybersecurity, there is good and bad news. The good news is that a majority of organizations continue to invest in cybersecurity, as ESG research indicates that more than 70% of Western European organizations expect to increase their security budgets in 2021.* The bad news? This ESG research project reveals that between 45% to 60% of European executives are only somewhat involved or not very involved in many critical cybersecurity activities. For example, 60% of these executives are somewhat involved or not very involved in reviewing metrics and KPIs across the entire security program. So, while organizations are investing in cybersecurity, executive teams know little about ROI on security technologies.

The data also reveals an alarming trend that executives are only somewhat involved, not very involved, or not at all involved in establishing a cybersecurity culture at their organization. Lacking this, cybersecurity will remain a technology-centric requirement rather than a crucial aspect of a 21st century business. This situation will only improve if business executives champion cybersecurity throughout the organization, where every employee believes they have a role in protecting the organization. This starts at the top, driven by CEOs and corporate directors.

Level of executive involvement in cyber activities.



**There is plenty
of room for
improvement.**

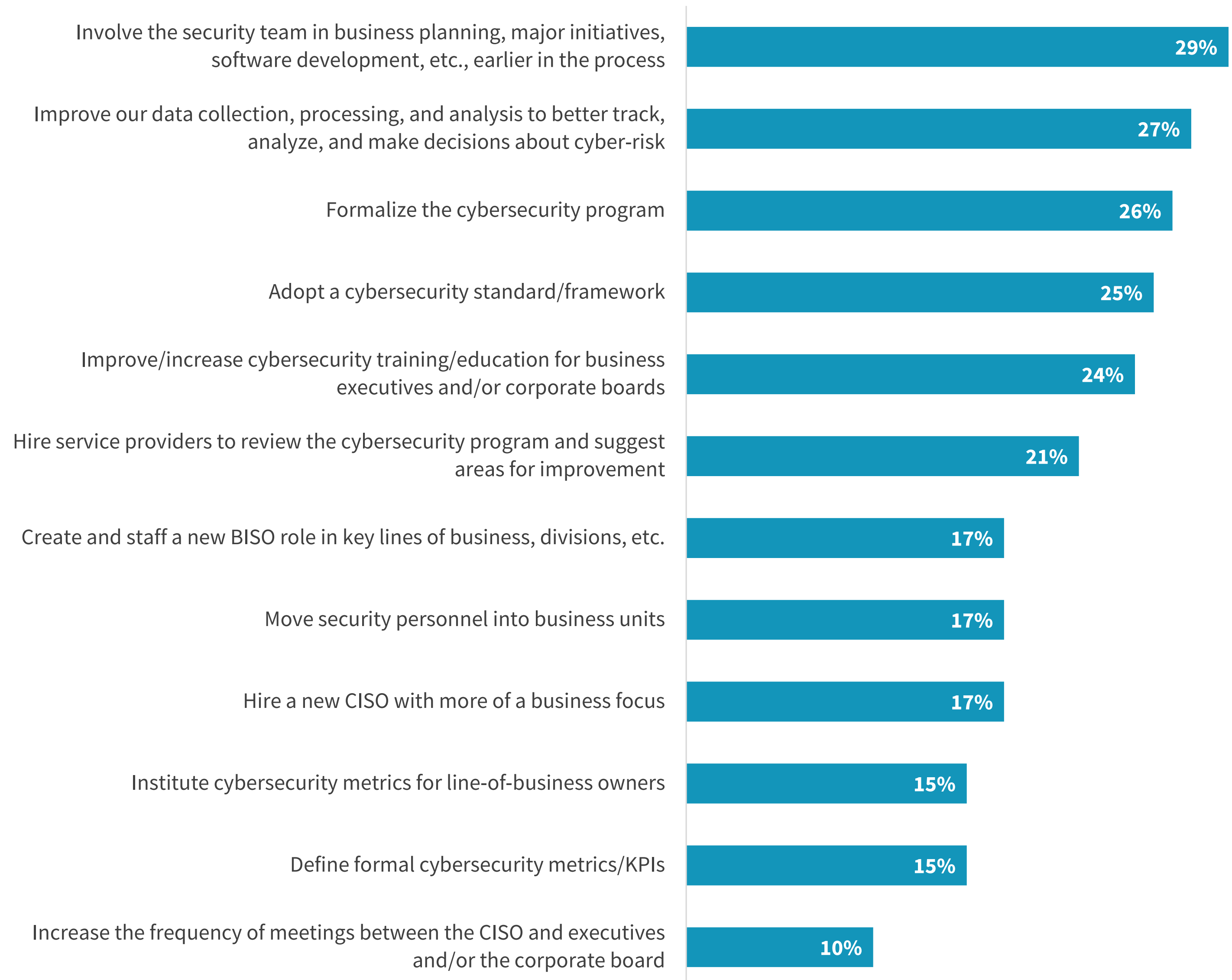


What Can Be Done to Improve Cybersecurity Alignment with the Business?

When it comes to the relationship between cybersecurity and the business, results are mixed. Corporate boards and executives are more educated and involved than they were in the past while CISOs are more actively participating in business planning and strategy. Alternatively, business executive and board involvement in cybersecurity seems cursory at best at most organizations.

European respondents pointed to numerous ways for their organizations to bridge the business/cybersecurity gap. For example, 29% suggested getting the security team more involved with business planning and major IT initiatives earlier in the process, 27% proposed improving data collection, processing, and analysis to improve cyber-risk management, and 24% recommended improving/increasing cybersecurity training/education for business executives and corporate boards.

Actions likeliest to improve cybersecurity and business alignment.





Recommendations



INSTITUTE THE RIGHT REPORTING STRUCTURE.

Fifty-six percent of European CISOs report to CIOs while 25% report to CEOs. Through its data analysis, ESG discovered that a CISO to CEO reporting structure is a best practice for leading organizations. This makes sense as a direct reporting structure means more cybersecurity exposure for CEOs and more business input for the cybersecurity team. Thus, this is a good place for organizations to start.



FORMALIZE THE CYBERSECURITY PROGRAM.

Too many cybersecurity programs are haphazard and technically focused. To align cybersecurity and the business, cybersecurity programs must be top-down, formalized and documented, and highlighted by KPIs and established metrics. This will help CISOs better communicate with business executives about the role of cybersecurity in the business using a common language.



EMPLOY BISOs.

Note that 17% of organizations say that they would better align cybersecurity and the business by creating a BISO role in key LOBs and divisions. ESG agrees. A business executive with cybersecurity knowledge could drive security at a granular level into business processes, critical assets, sensitive data, and employee roles. This would also help align security with business productivity.



Trend Micro, a global leader in cybersecurity, helps make the world safe for exchanging digital information. Leveraging over 30 years of security expertise, global threat research, and continuous innovation, Trend Micro enables resilience for businesses, governments, and consumers by providing connected security across the IT infrastructure.

[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.

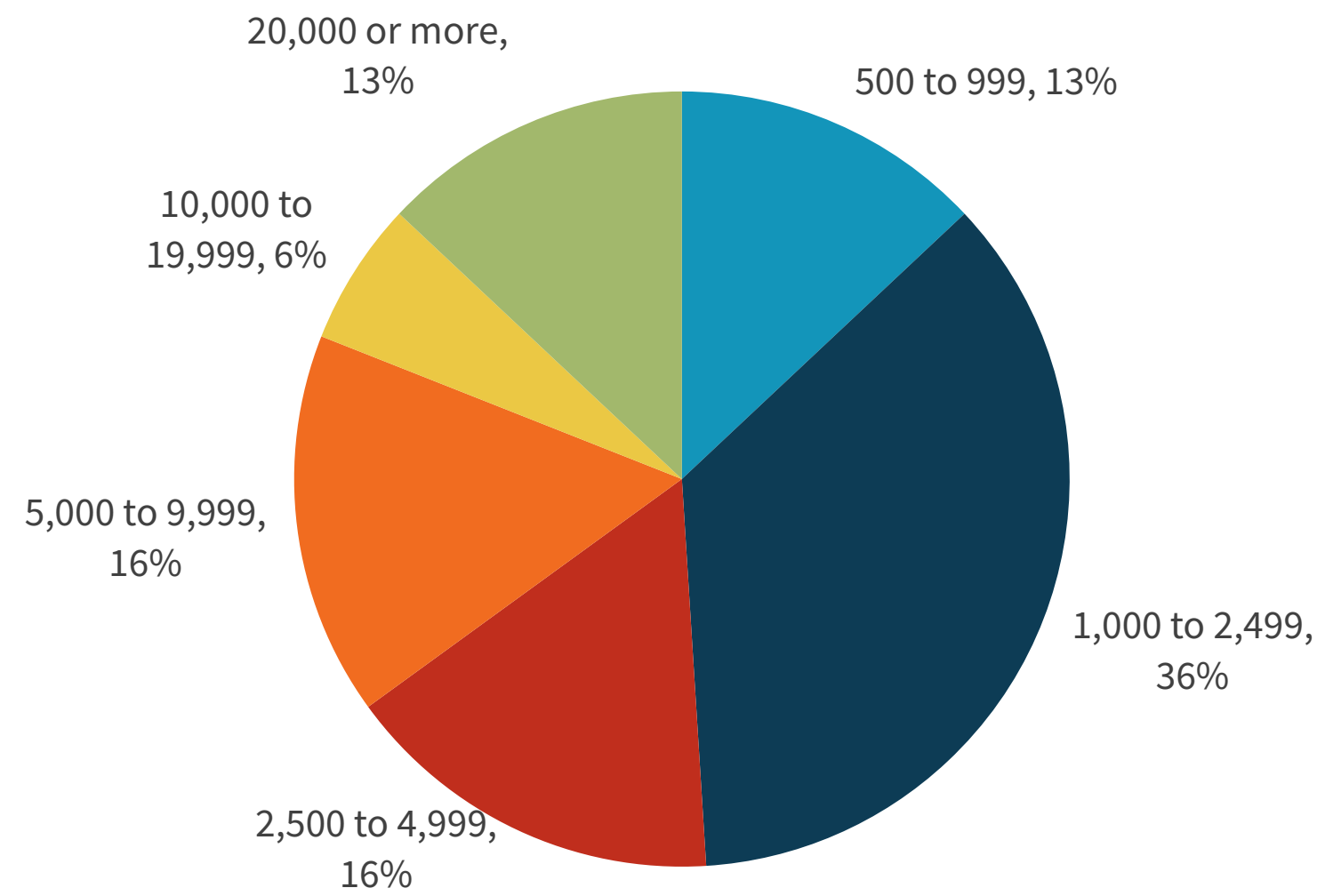


Research Methodology

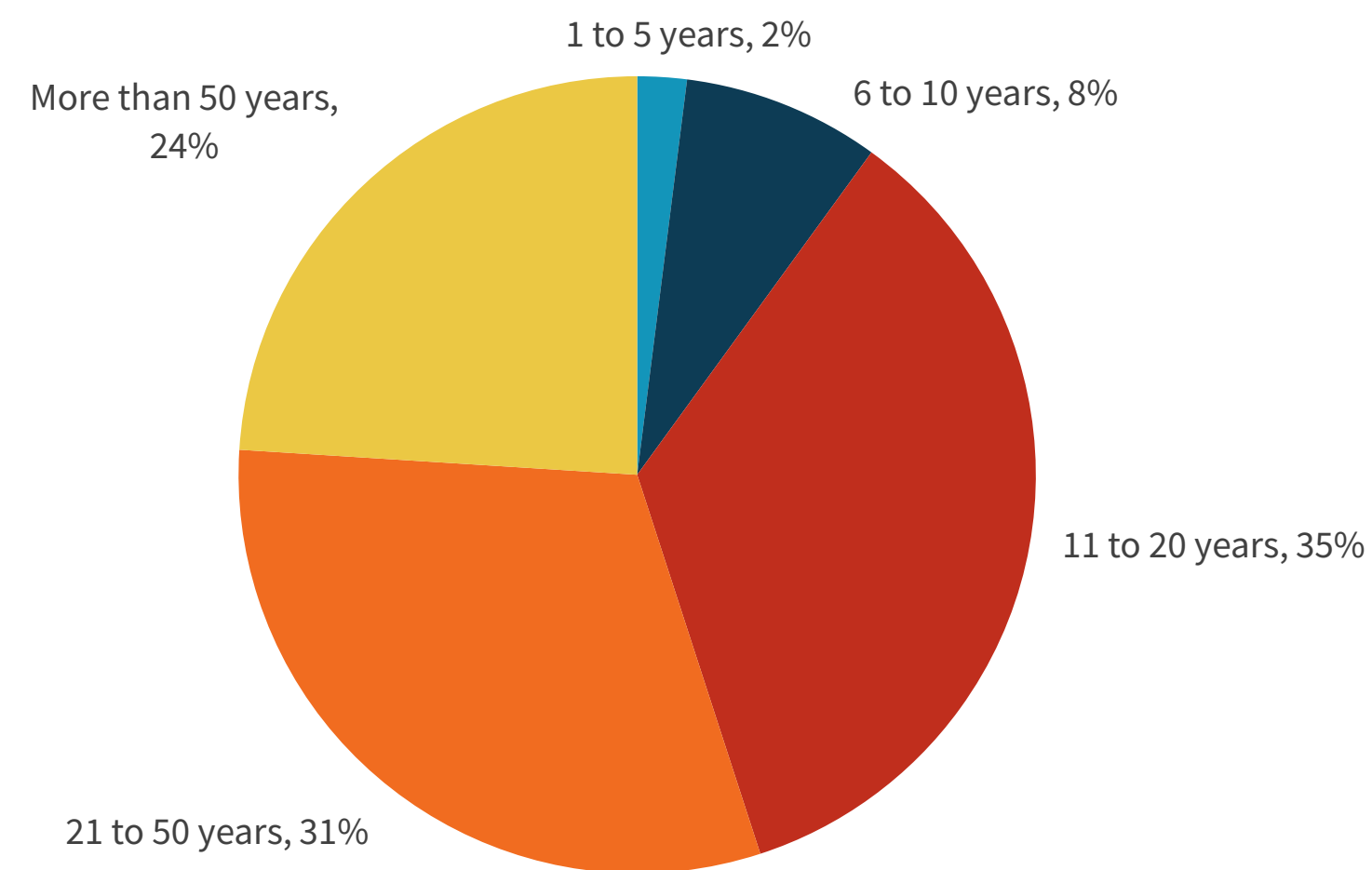
To gather data for this report, ESG conducted a comprehensive online survey of senior business, cybersecurity, and IT professionals from private- and public-sector organizations in Western Europe (UK, France, and Germany) between September 28, 2020 and October 24, 2020. To qualify for this survey, respondents were required to be senior business, cybersecurity, and IT professionals personally responsible for or familiar with their organization’s environment and strategy. 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 100 senior business, cybersecurity, and IT professionals.

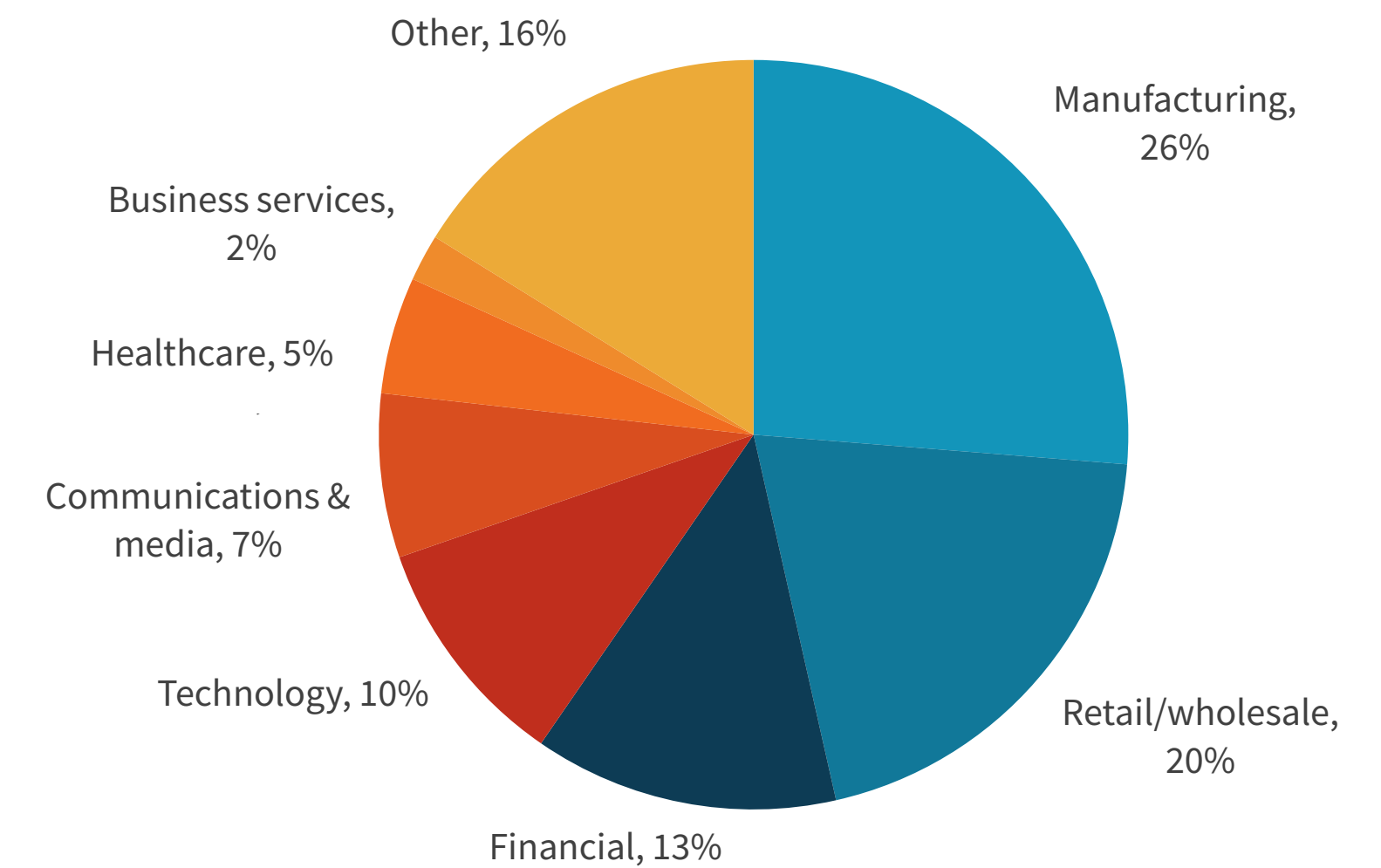
RESPONDENTS BY NUMBER OF EMPLOYEES



RESPONDENTS BY AGE OF COMPANY



RESPONDENTS BY INDUSTRY



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 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 market intelligence and actionable insight to the global IT community.

© 2021 by The Enterprise Strategy Group, Inc. All Rights Reserved.