Enterprise Strategy Group™
by TechTarget

Midmarket and Small Enterprise Cybersecurity Program Development: A Work in Progress

Dave Gruber | Principal Analyst

ENTERPRISE STRATEGY GROUP

SEPTEMBER 2024

Research Objectives

Despite their need for comprehensive cybersecurity programs, midmarket and small enterprise organizations often have limited budgets and resources, making attracting skilled personnel challenging for these firms. Gaps in security visibility, policies, processes, and infrastructure plus a tendency to use older systems and software make these organizations more vulnerable to attack than businesses with more mature and better funded cybersecurity cultures.

Even with continued successful cyberattacks across industries, midmarket and small enterprise organizations frequently fail to react quickly or sufficiently to threats, accepting risk without understanding the potential impact. Highly dependent on third-party SaaS applications and infrastructure, smaller companies often lack visibility into operational threat signals, resulting in an excessive progression of attacks before discovery.

To further assess and understand the current state of cybersecurity programs at these smaller organizations, TechTarget's Enterprise Strategy Group surveyed 379 IT and cybersecurity professionals at midmarket and small enterprise organizations in North America (US and Canada).

THIS STUDY SOUGHT TO:

Define the security needs and preferred strategies of midmarket and small enterprise organizations.

Explore the current state of security program development.

Identify key gaps and challenges associated with security programs.

Understand desired operating models and categorize the most common types.

KEY FINDINGS

Despite a Critical Dependence on IT, Almost Half of Midmarket and Small Enterprises Feel Vulnerable

PAGE 4

Cybersecurity Program Strategy Is a Work in Progress for Most

PAGE 10

Hybrid SOC Operating Models Are Helping, but More Work Is Required

PAGE 17

Consolidated Cybersecurity Solutions Are Preferred, but Specialty Solutions Are Still Needed

PAGE 21

> “90% of midmarket and small enterprise organizations feel that technology **plays a critical role** in their operating infrastructure.”

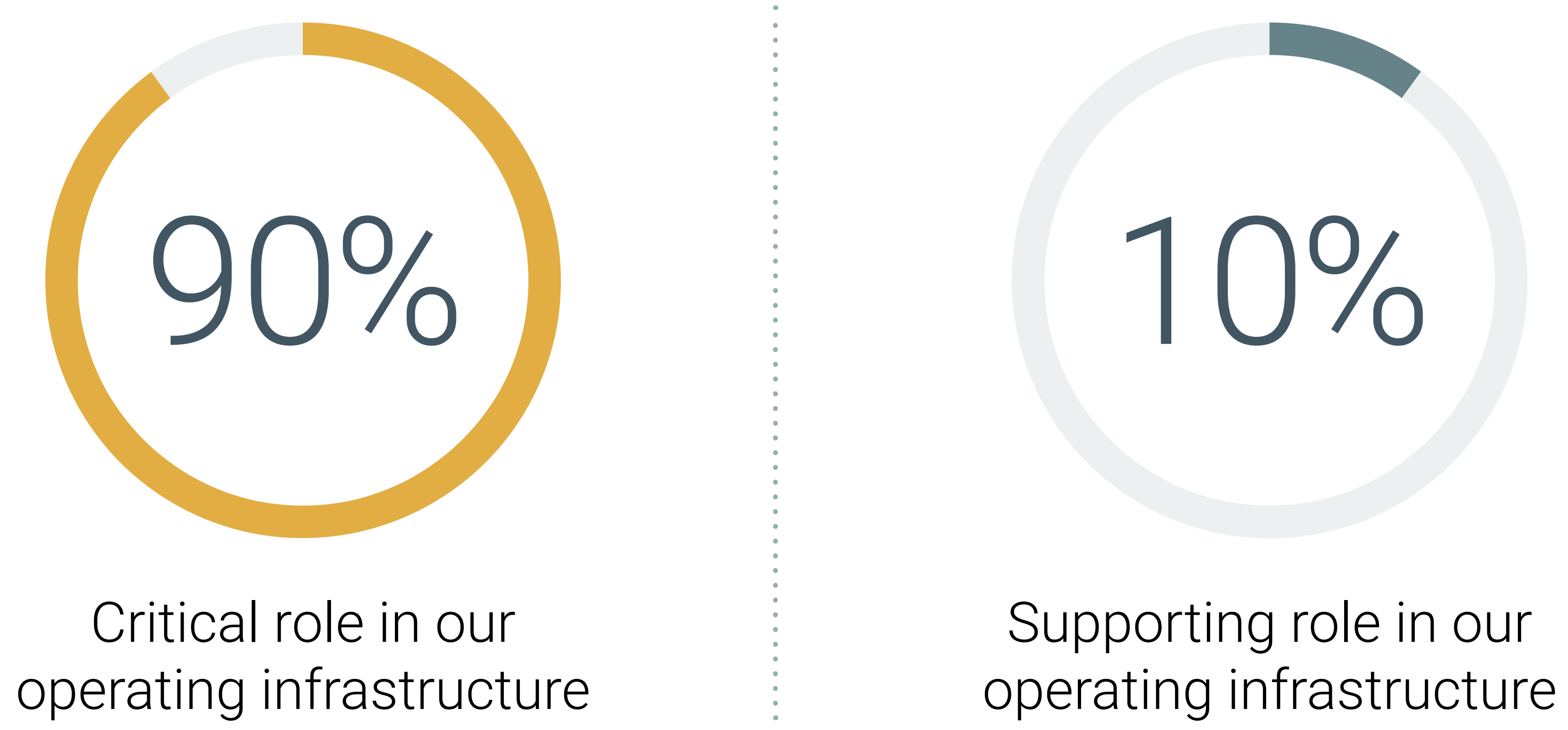
Dave Gruber | Principal Analyst
ENTERPRISE STRATEGY GROUP

Despite a Critical Dependence on IT, Almost Half of Midmarket and Small Enterprises Feel Vulnerable

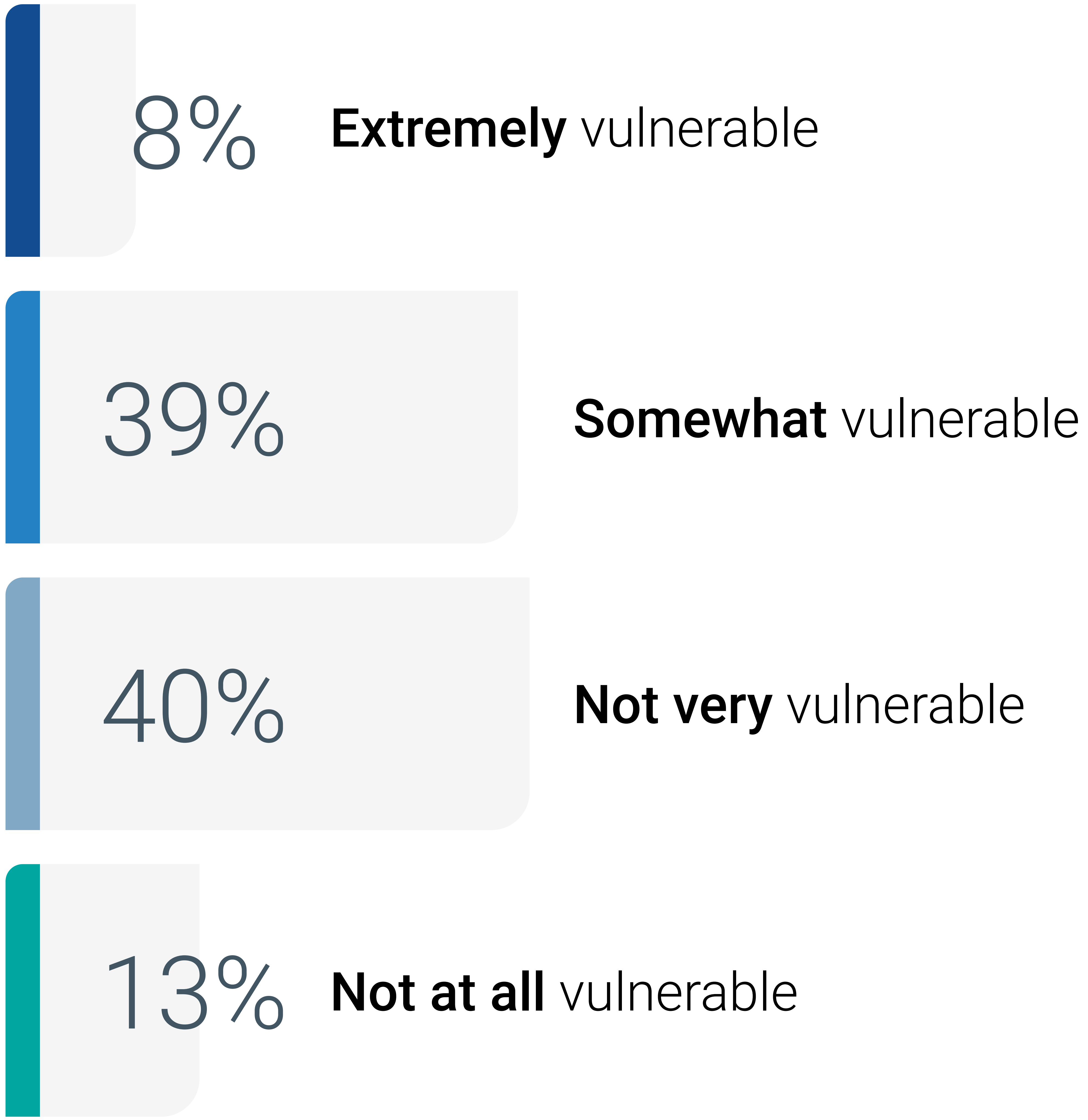
The Critical Role of IT Infrastructure and the Associated Vulnerability

According to the research, 90% of midmarket and small enterprise organizations feel that technology plays a *critical* role in their operating infrastructure, leaving many at risk of disruption from cyberattacks. Indeed, when it comes to attacks that disrupt business processes or lead to theft of sensitive data, nearly half report they are either extremely (8%) or somewhat (39%) vulnerable to significant cyberattacks or data breaches.

Role that technology plays in organizations' ability to support business operations and achieve desired business outcomes.



How vulnerable organizations believe they are to a significant cyberattack or data breach.



BACK TO CONTENTS

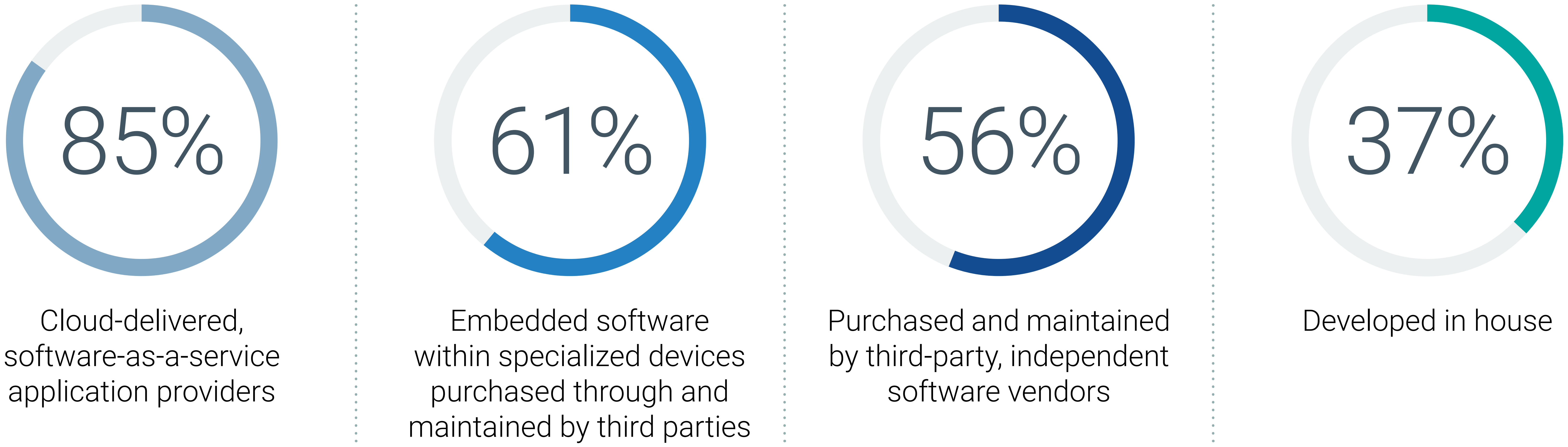
SaaS Application Use Prevails

When asked about their most important applications, 85% of organizations confirmed that they procure them as cloud-delivered, SaaS applications. Additionally, nearly two-thirds leverage embedded software within specialized devices purchased through and maintained by third parties.

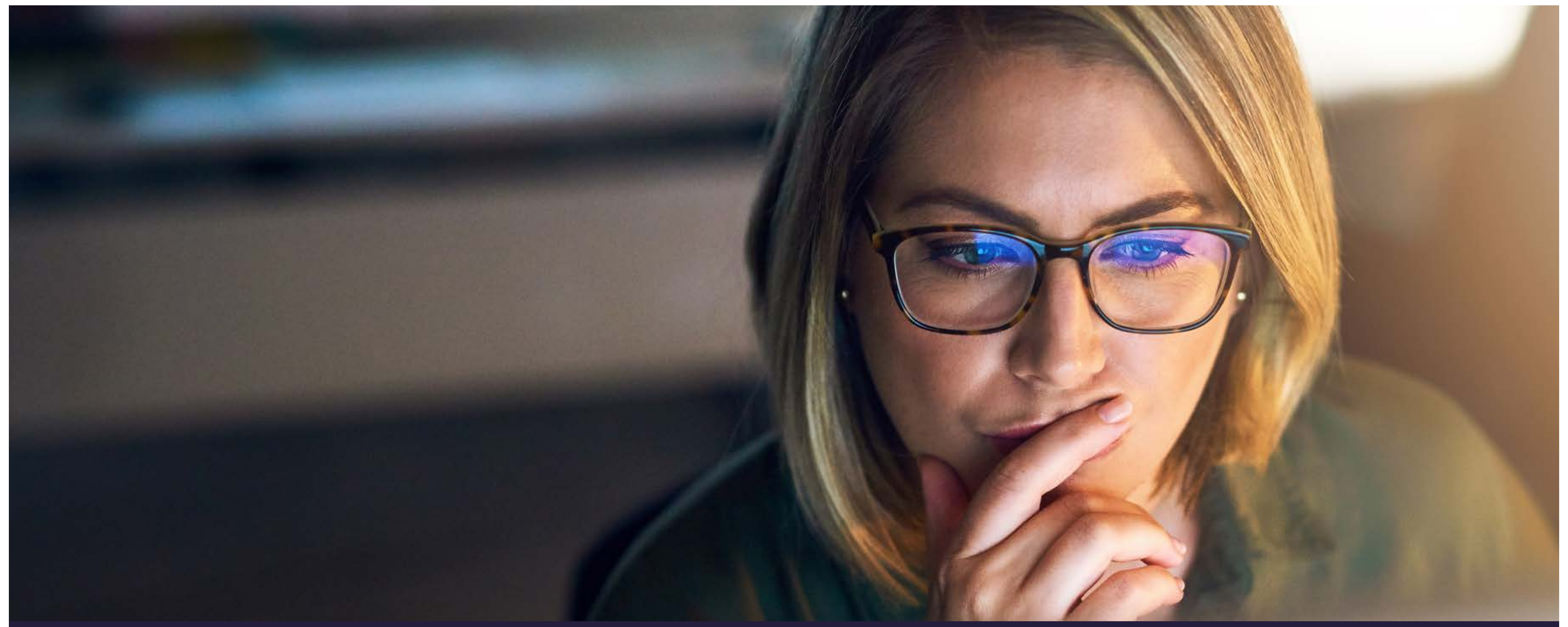
With limited budget and resources applied to IT and cybersecurity at these organizations, these operating models provide rapid access to modern application infrastructure without requiring significant capital investment, in addition to offering a scalable infrastructure that can support growth and scale over time.

It is worth noting that only 37% of midmarket and small enterprise organizations develop their most important applications in house.

How organizations currently procure their most important applications.



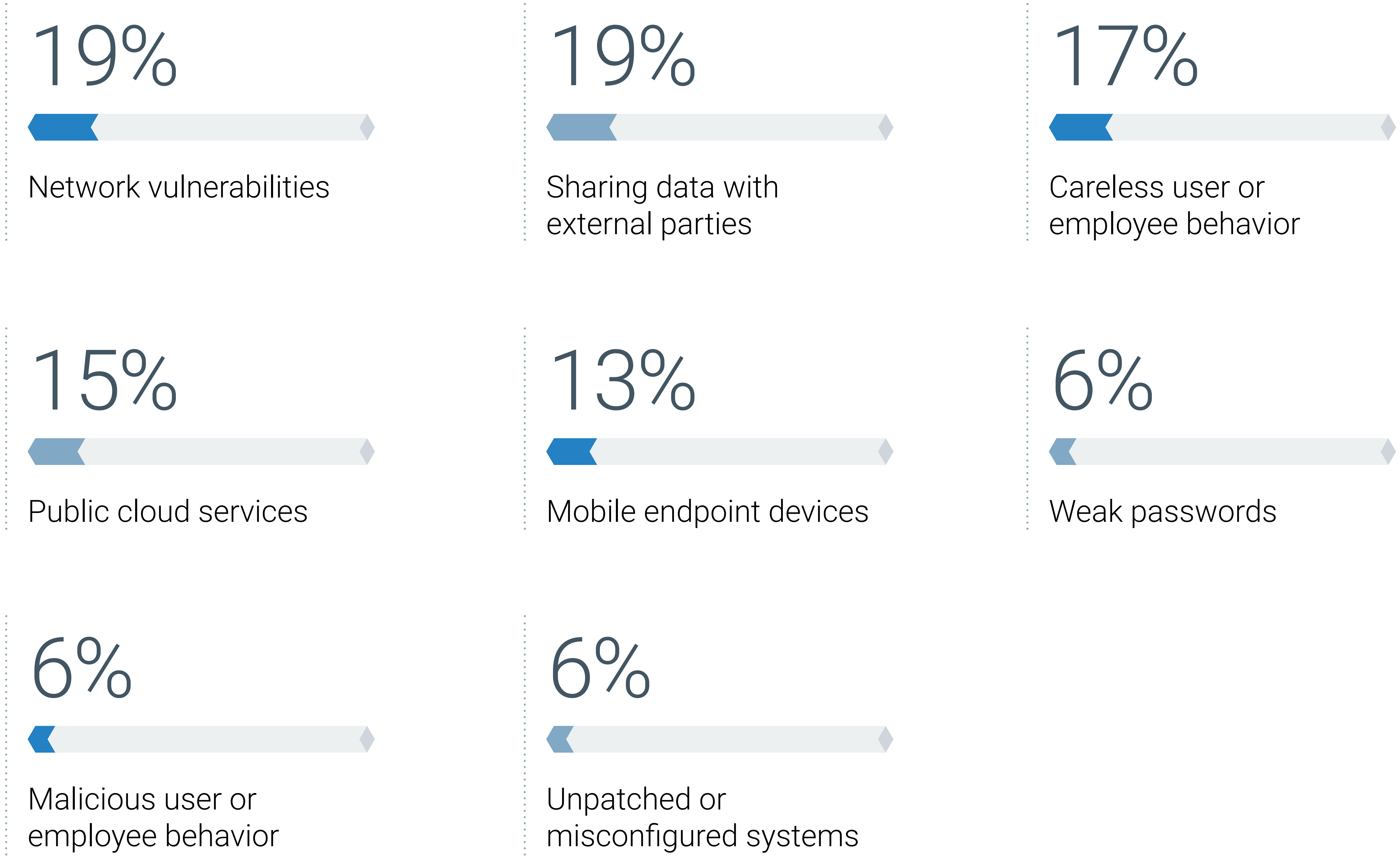
> "Nearly two-thirds leverage embedded software within specialized devices purchased through and maintained by third parties."



Where Are Smaller Organizations Most Vulnerable?

In support of the use of as-a-service applications, smaller organizations require stable and secure network infrastructure to provide access. This critical piece of infrastructure is therefore where small organizations feel highly vulnerable, ranking network vulnerabilities at the top of potential breach points. Equally ranked at the top is the common practice of sharing data with external parties, as loss of control leaves many feeling worried about sensitive information.

Organizations' single biggest cybersecurity vulnerability and potential breach point.



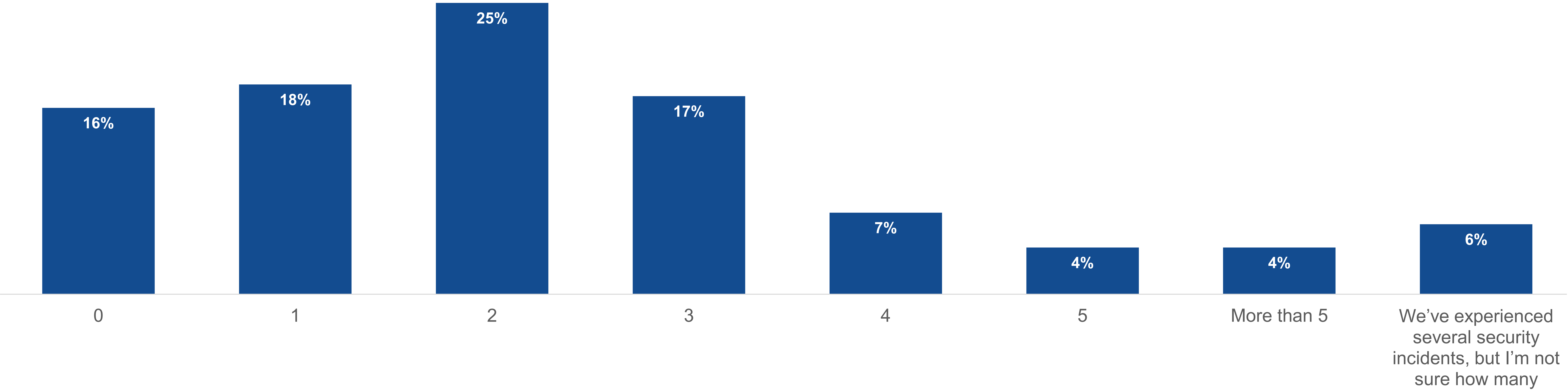
Security Incidents Experienced in the Last 24 Months

With nearly two-thirds (63%) reporting they have experienced two or more security incidents over the past two years, strengthening cybersecurity strategies is a priority for most. Indeed, 83% plan to increase investments in cybersecurity operations technologies, services, and personnel in the coming 12 months.

83%

plan to **increase investments in cybersecurity operations technologies, services, and personnel** in the coming 12 months.

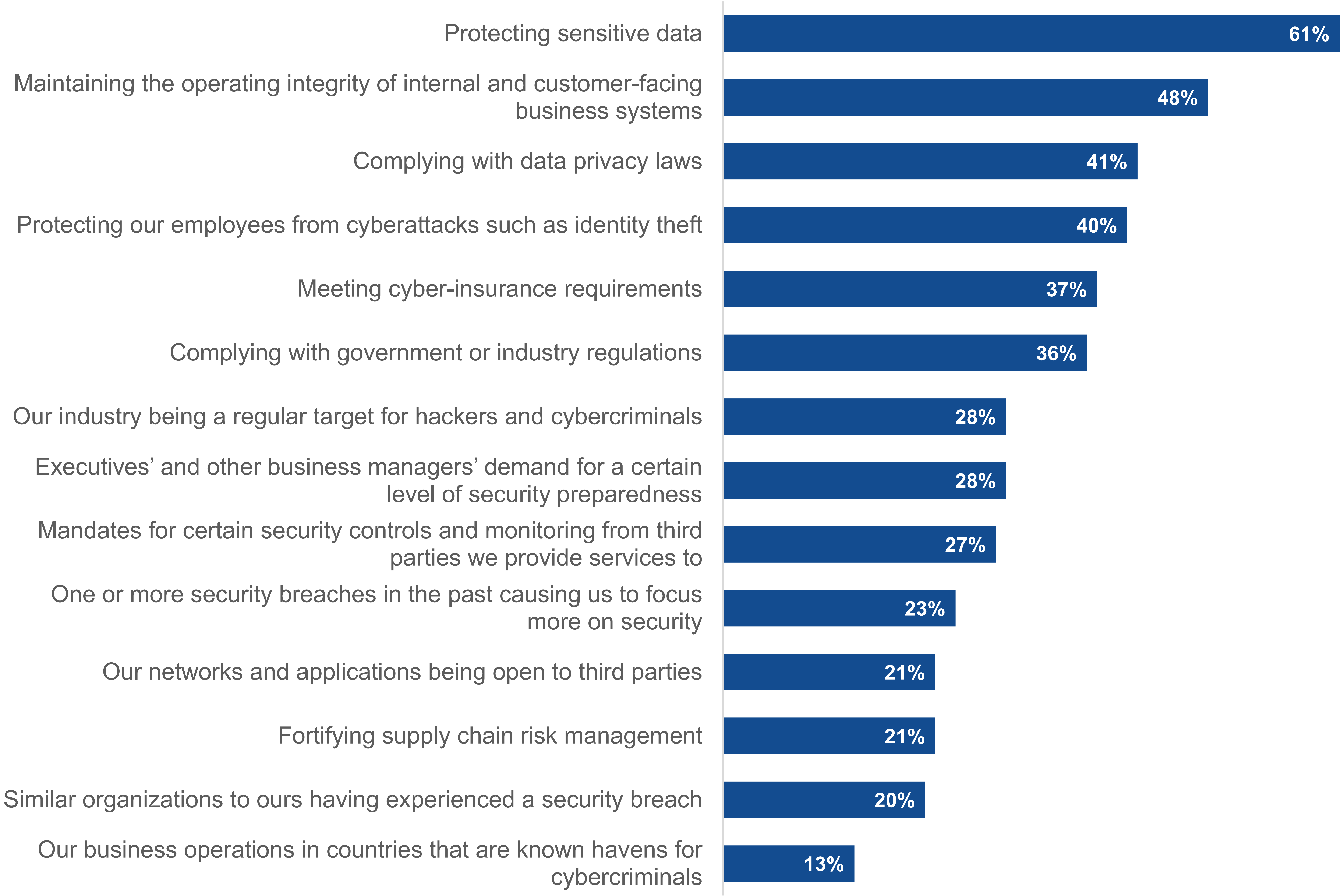
Number of times organizations have experienced a security incident over the past two years.



Cybersecurity Program Drivers: What's Most Important

Key cybersecurity program drivers for this audience include protecting sensitive data and maintaining the operating integrity of internal and customer-facing business systems. Compliance objectives such as obeying privacy laws, complying with government or industry regulations, and meeting cyber-insurance requirements also are leading drivers.

Key drivers for organizations' cybersecurity programs.

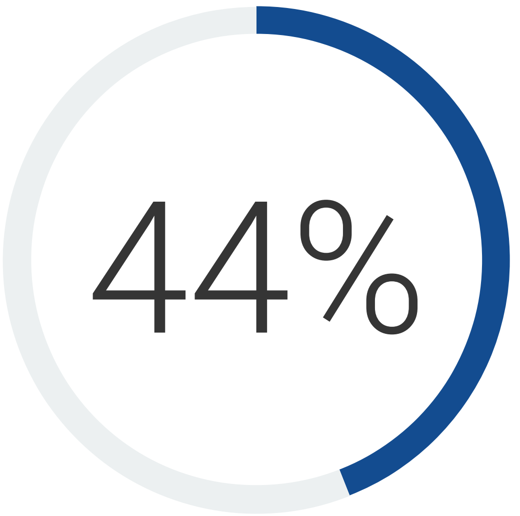


Cybersecurity Program Strategy Is a Work in Progress for Most

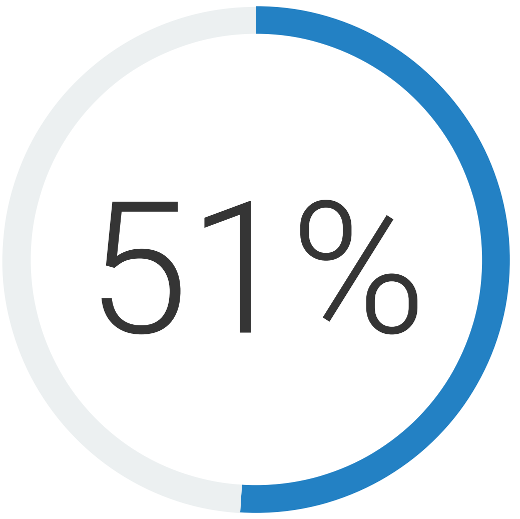
Level of Cybersecurity Program Maturity

While more cybersecurity program investments and strategy refinements are planned, 44% already think that their cybersecurity program is in a mature state. That said, the remaining 55% of organizations report that cybersecurity program strategies are still a work in progress.

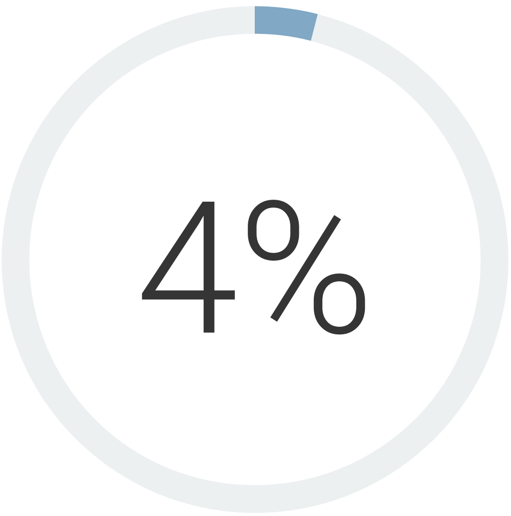
Current state of organizations' cybersecurity programs.



Mature - cybersecurity program strategies are developed, implemented, and fully operational



Developing - most program strategies have been developed but are still a work in progress

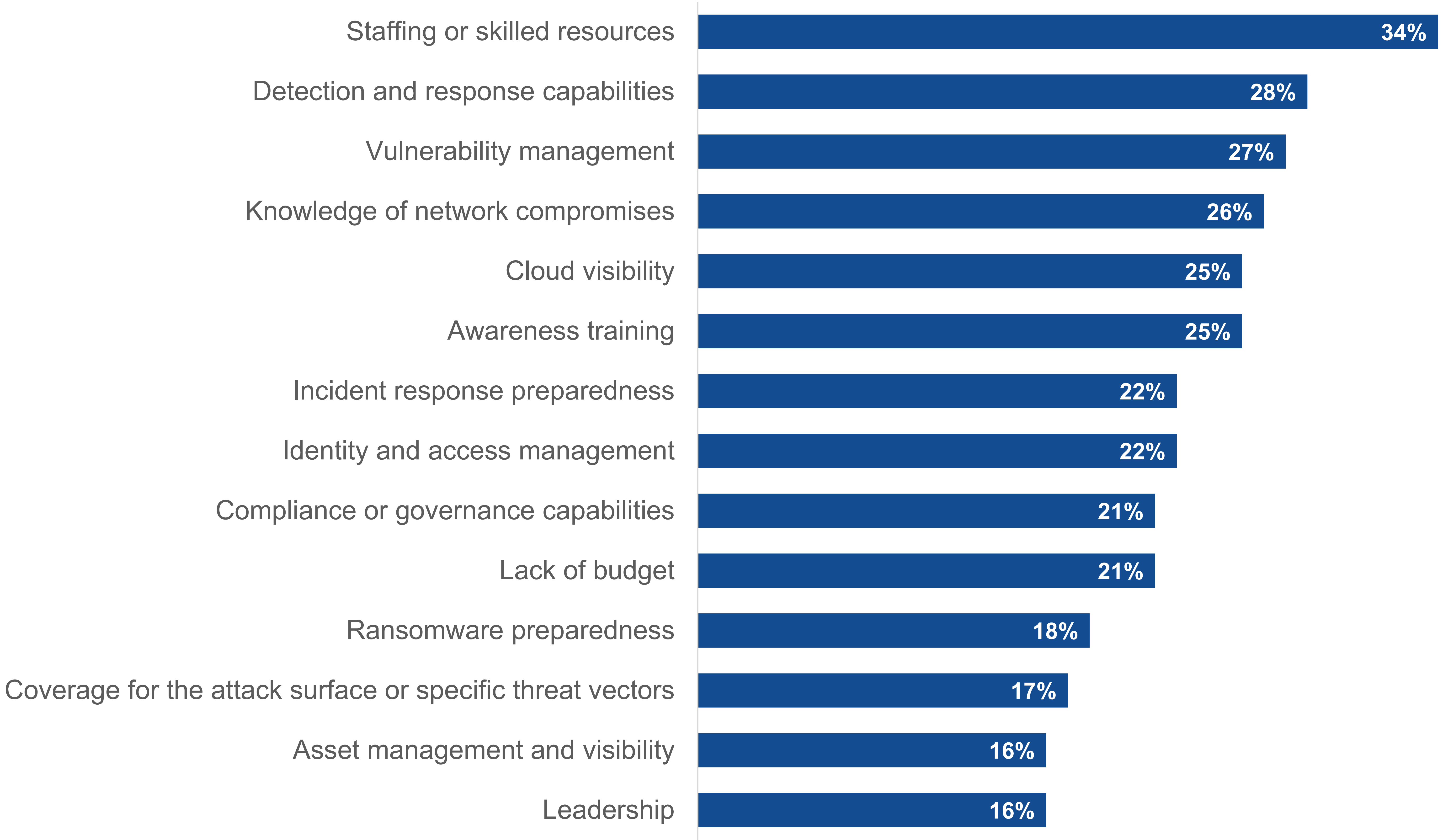


Aspiring - many program strategies are nascent and still evolving

Biggest Cybersecurity Program Gaps

Like larger organizations, midmarket and small enterprise organizations are impacted by the global cybersecurity skills shortage, ranking staffing and/or finding skilled resources at the top of the list of biggest program gaps. Also similar to large organizations, gaps in detection and response capabilities, vulnerability management, and network visibility top the list, along with gaining cloud visibility and adequate levels of security awareness training for workers.

Biggest gaps within organizations’ current security programs.



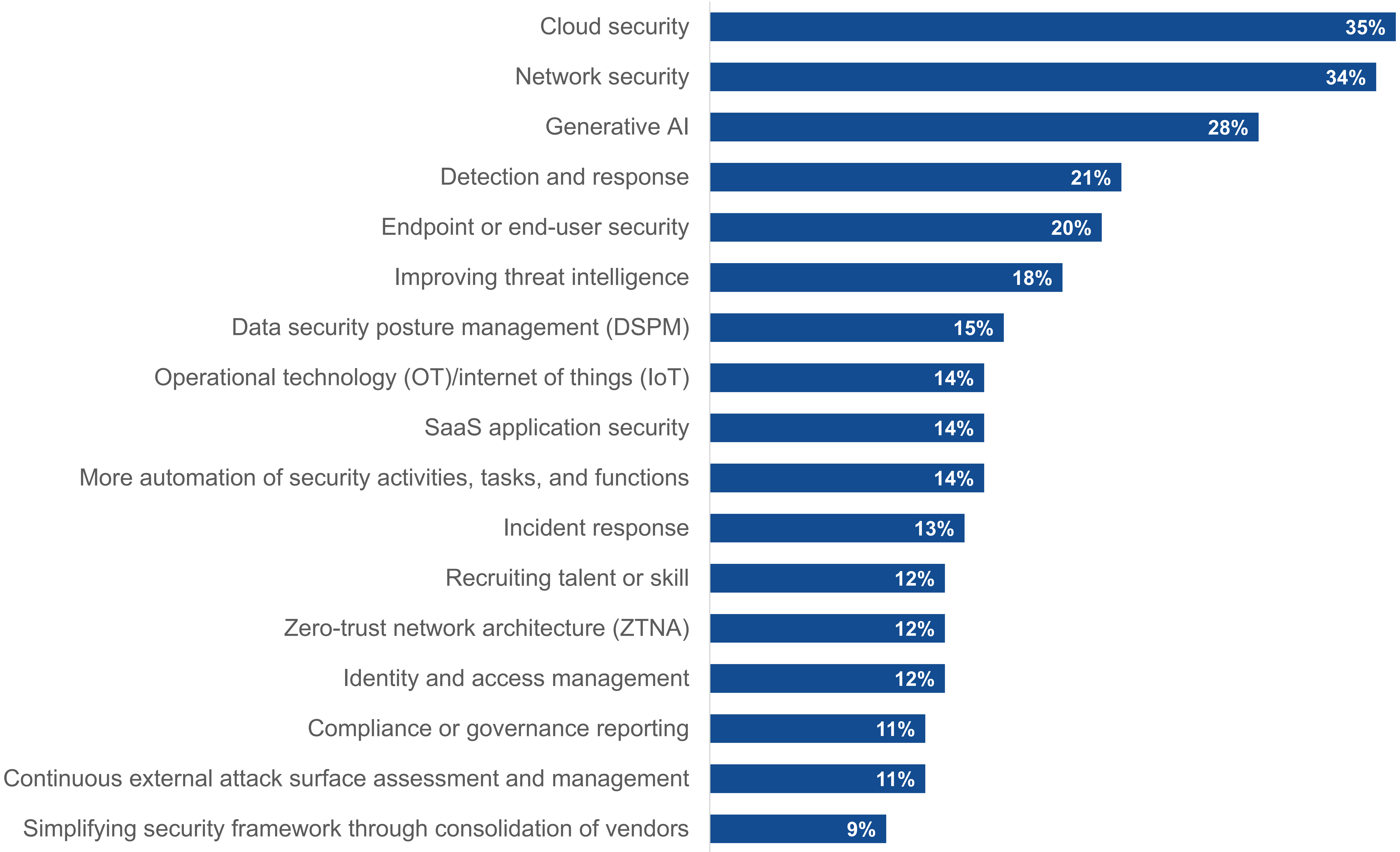
Closing the Gaps: Where Is the Focus?

Given the previously identified cybersecurity program gaps, where are midmarket and small enterprise organizations focused?

Based on the market-wide prevalence of SaaS application usage, it's no surprise to see cloud and network security at the top of the list. Generative AI has caught the attention of these organizations with more than a quarter identifying it as an area of mindshare for their security teams.

Beyond the top three, other areas of focus include improving detection and response, endpoint or end-user security, and threat intelligence.

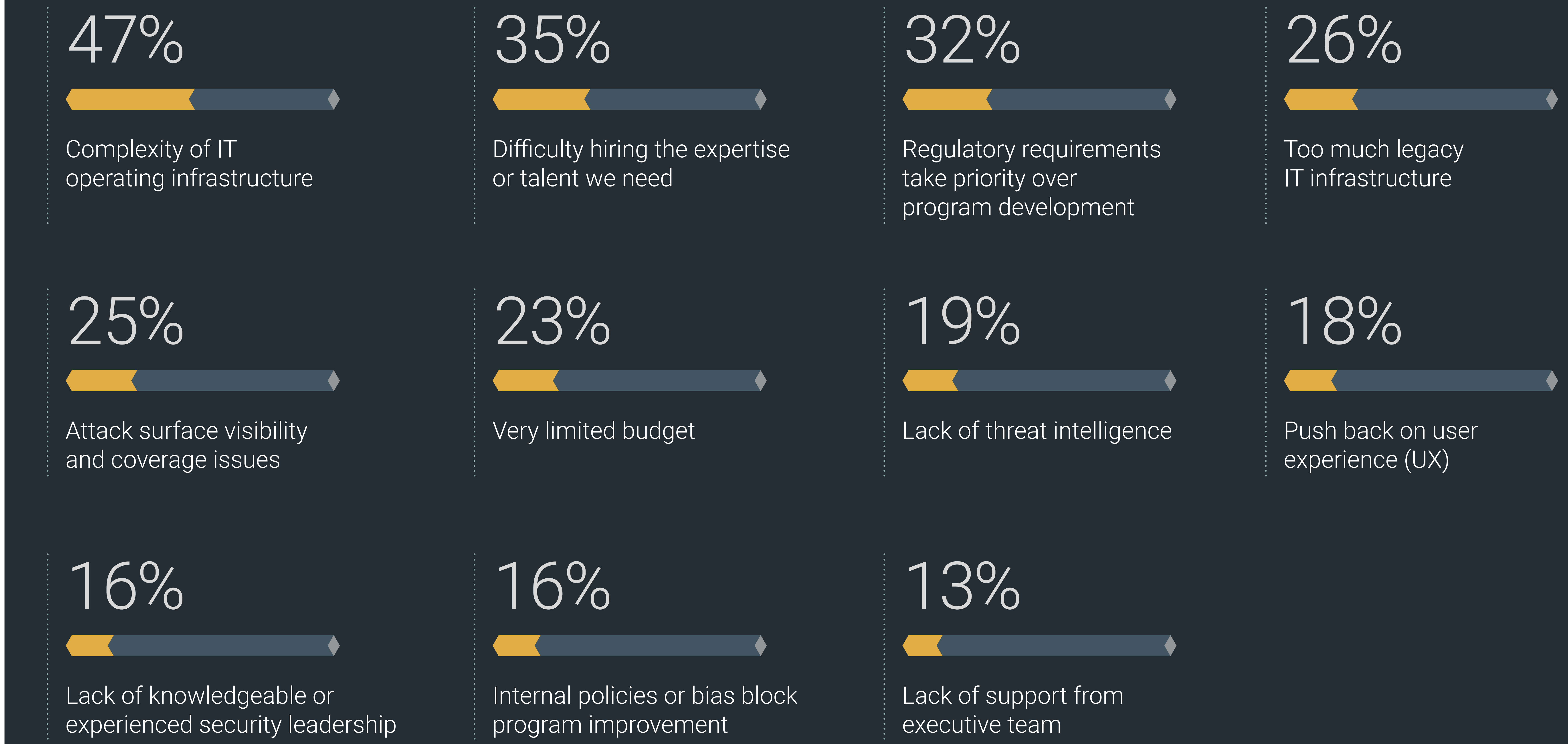
Cybersecurity-related topics that are the biggest areas of focus for security teams.



Common Program Constraints: ‘The World We Live in’

While program development issues overlap with those often faced by larger organizations, such as the complexity of IT operating infrastructure, small organizations need to navigate through constraints in building and managing their cybersecurity programs that larger organizations do not. Constraints include more difficulty in hiring the expertise and talent needed and prioritizing regulatory requirements over security program development.

Constraints organizations deal with building, refining, and managing their cybersecurity program.

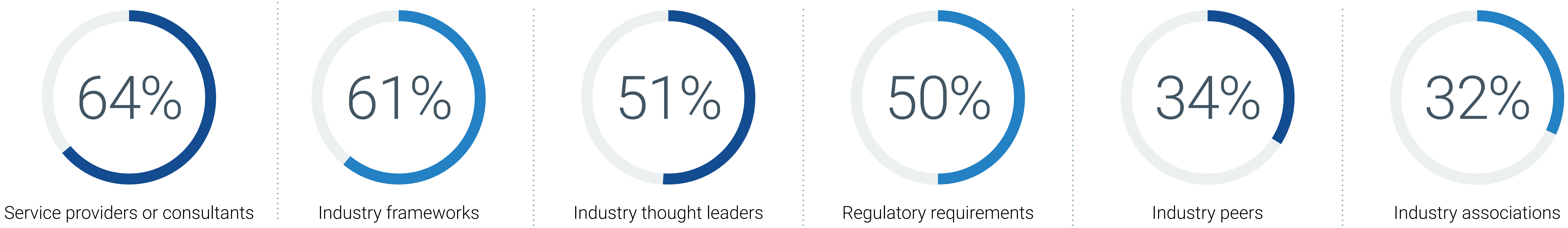


47%	Complexity of IT operating infrastructure
35%	Difficulty hiring the expertise or talent we need
32%	Regulatory requirements take priority over program development
26%	Too much legacy IT infrastructure
25%	Attack surface visibility and coverage issues
23%	Very limited budget
19%	Lack of threat intelligence
18%	Push back on user experience (UX)
16%	Lack of knowledgeable or experienced security leadership
16%	Internal policies or bias block program improvement
13%	Lack of support from executive team

Who Helps Guide Program Strategy?

So where are cybersecurity leaders within these midmarket and small enterprise organizations getting help and guidance as they strive to overcome program gaps and constraints? Nearly two-thirds (64%) turn to managed security service providers or consultants for guidance on program development. Industry frameworks, industry thought leaders, and regulatory requirements further guide strategies.

Where cybersecurity leaders look for guidance on security program development.



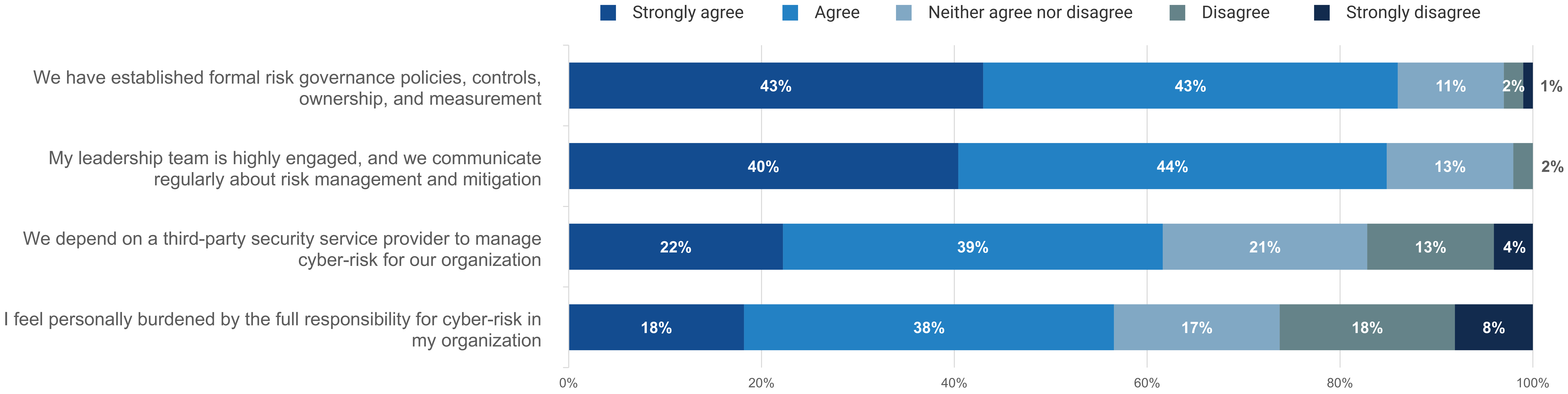
BACK TO CONTENTS

Risk Management Processes

As IT and security leaders strive to align cybersecurity programs with broader risk-management objectives, 86% report having established, formal risk governance policies, controls, ownership, and measurement. Additionally, 84% report that their leadership team is highly engaged, and that they communicate regularly about risk management and mitigation.

More alarming, though, is that despite this level of engagement, more than half (56%) of cybersecurity leaders feel personally burdened by the full responsibility for cyber-risk in their organization.

Perspectives on risk management processes.



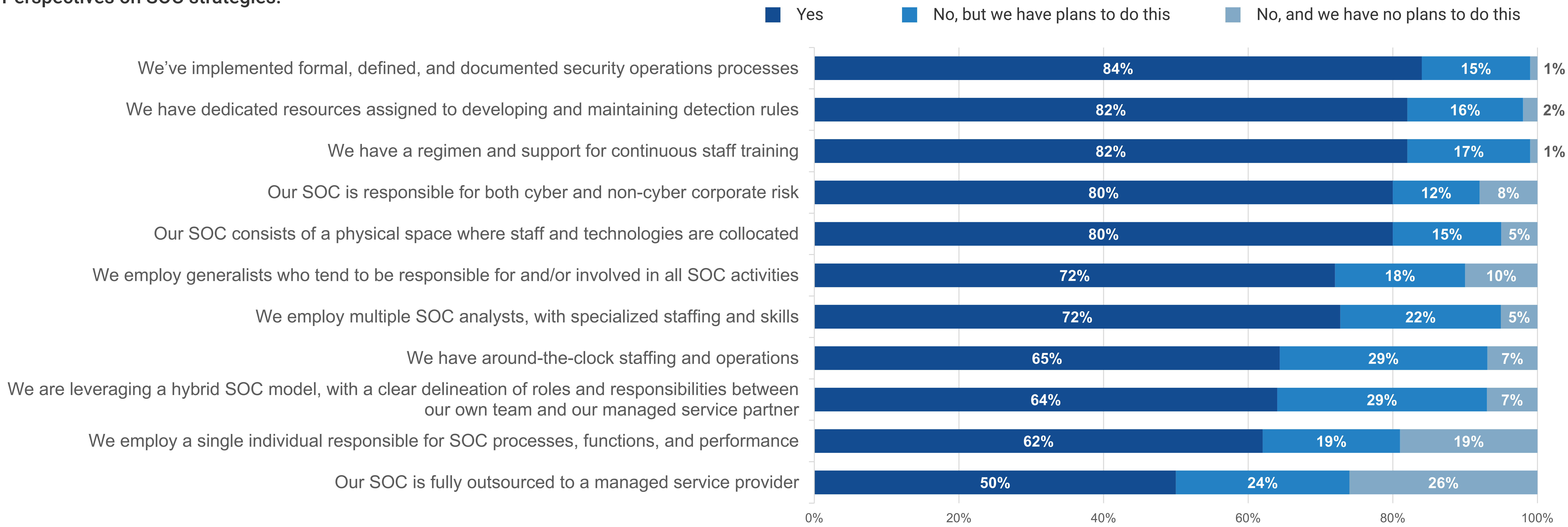
Hybrid SOC Operating Models Are Helping, but More Work Is Required

SOC Strategies

Despite feeling an intense burden of responsibility, cybersecurity leaders in midmarket and small enterprise organizations are not operating alone. Half have already fully outsourced their security operations center (SOC), with another 24% planning to outsource to a managed service provider. Neatly two-thirds (64%) leverage a hybrid SOC model, with a clear definition of roles and responsibilities between internal teams and managed service partners.

But in smaller organizations, personnel often “wear multiple hats,” with 80% reporting that their SOC is responsible for both cyber and non-cyber corporate risk.

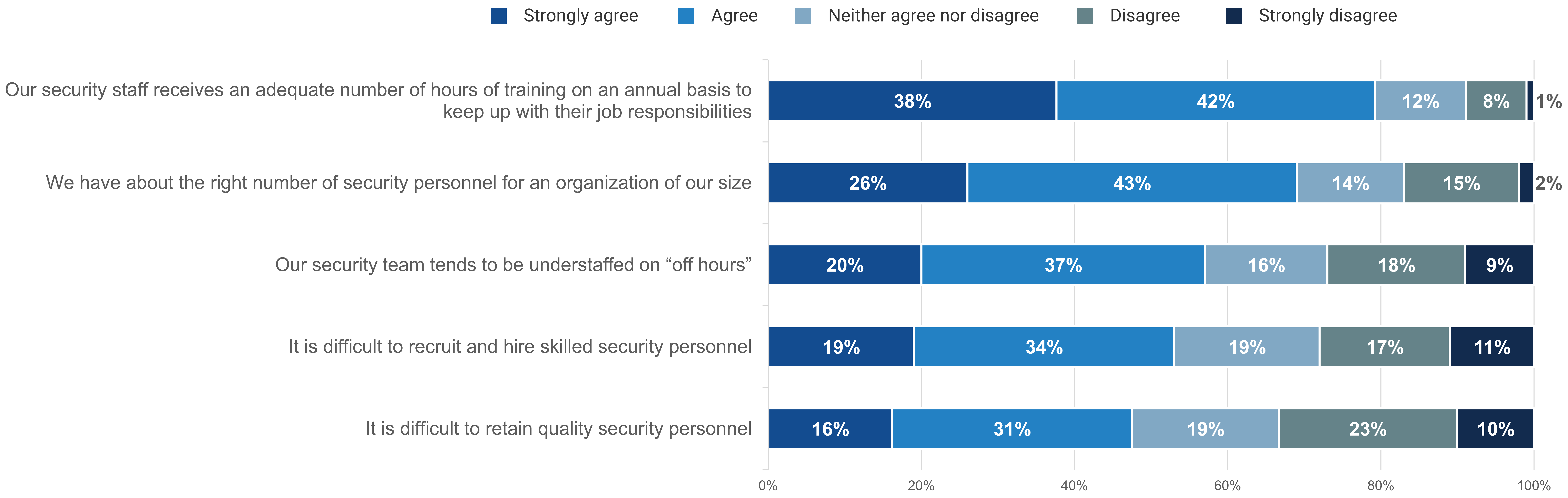
Perspectives on SOC strategies.



Cybersecurity Personnel

Despite staffing challenges, more than two-thirds (69%) actually report having about the right number of security personnel for an organization of their size. That said, 57% say that their teams tend to be understaffed on "off hours," with about half also reporting that they struggle to recruit, hire, and retain skilled security personnel.

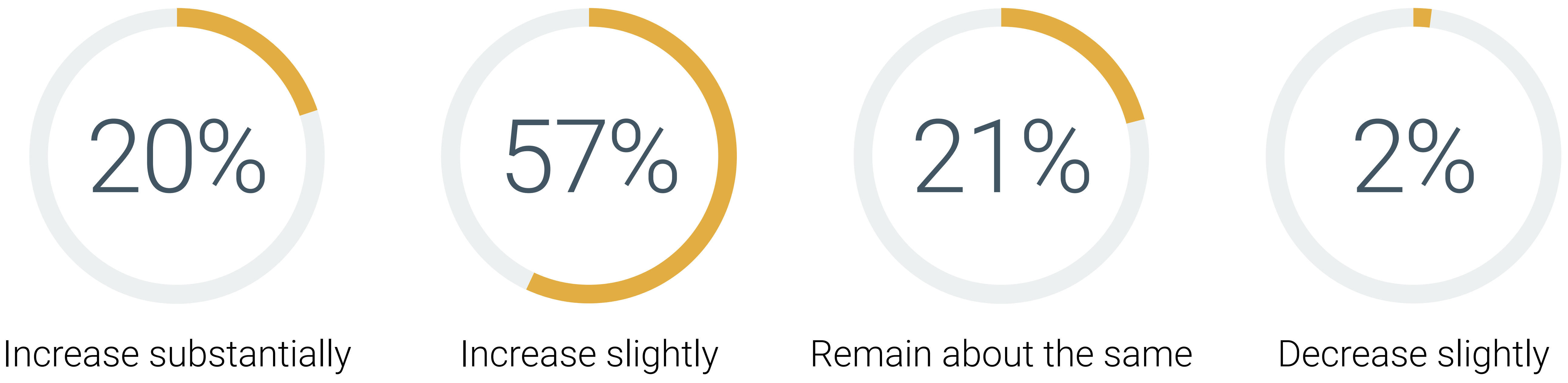
Perspectives on cybersecurity personnel.



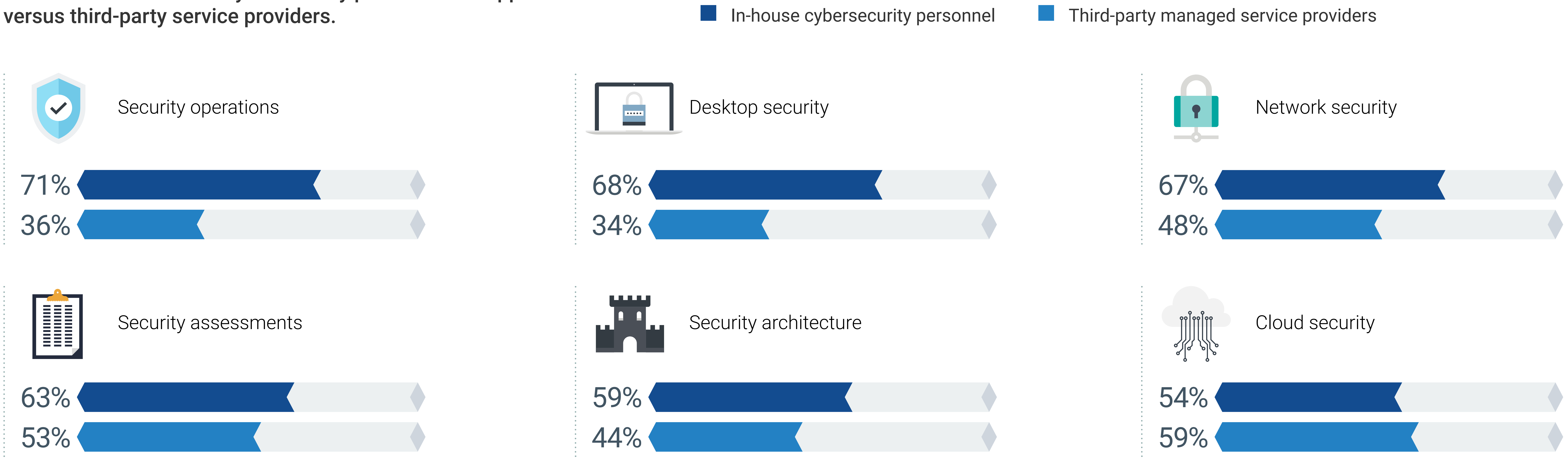
Third-party Services Widely Utilized, Together With Internal Staff

Hybrid operating models are the answer for most, combining internal security personnel with third-party managed service providers. This model supports most aspects of cybersecurity, including security operations; desktop, network, and cloud security; and more proactive security strategies such as assessments and architecture development. Looking ahead, usage of managed security services is expected to increase, with 77% planning to increase their use either substantially or slightly.

Expected change in the use of managed security services over the next 12-24 months.



Where current in-house cybersecurity personnel are applied versus third-party service providers.



BACK TO CONTENTS

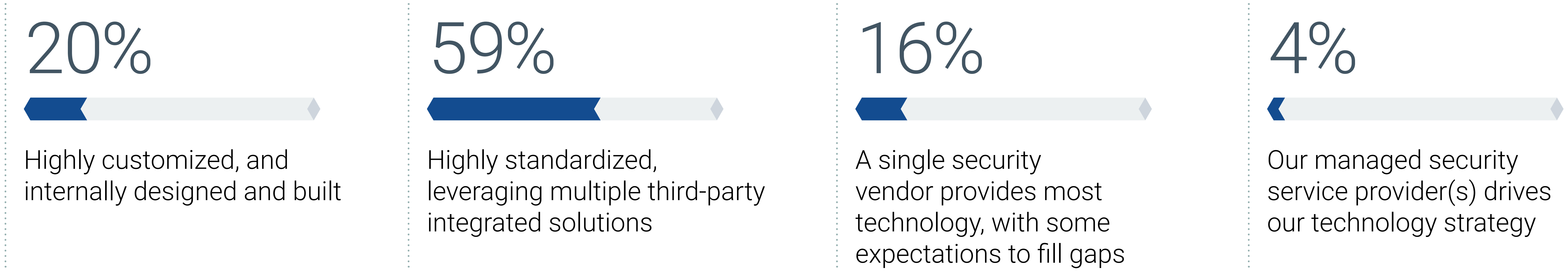
Consolidated Cybersecurity Solutions Are Preferred, but Specialty Solutions Are Still Needed

Most Use Multiple Third-party Solutions, Though From a Relatively Small Number of Providers

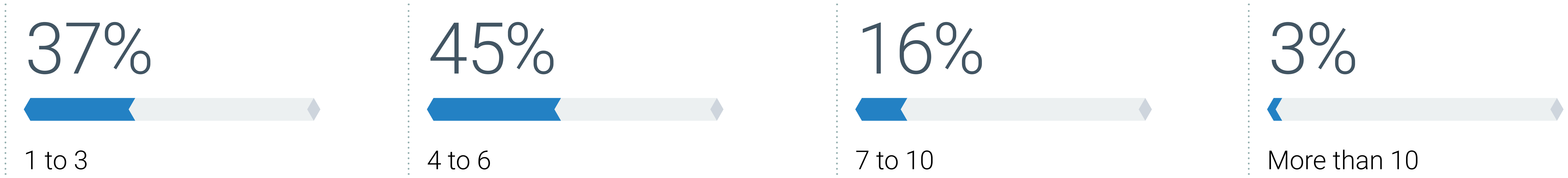
When it comes to the cybersecurity technology stack, smaller organizations often operate differently from large organizations. Most standardize on a security technology stack, but often still acquire solutions from multiple providers.

More than eight in ten organizations report utilizing six or fewer different cybersecurity technology solutions or service providers, whereas large enterprise organizations frequently utilize in excess of 20. This strategy keeps the complexity down, while reducing the cost of integrations and ongoing architectural management. Notably, this also reduces the need to invest in ongoing consolidation projects, as more integrated security solutions already take care of this.

Current security technology strategy.



Number of different cybersecurity technology solutions and/or service providers in use.



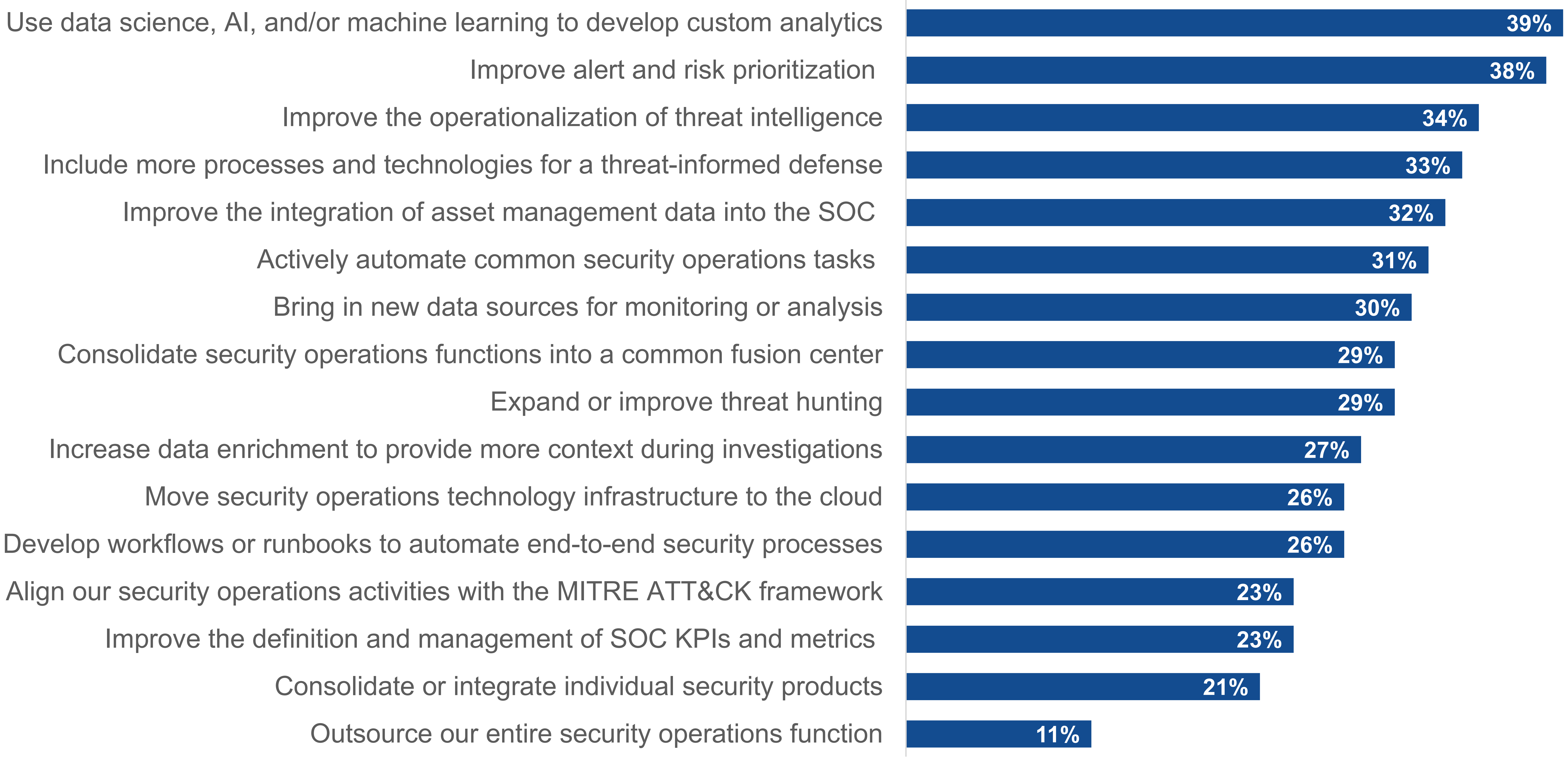
Where Are Security Leaders Focused Moving forward?

Despite the many differences in how large and small cybersecurity teams operate, many of the areas of leaders' focus for the coming year are aligned.

Like large-scale cybersecurity teams, smaller teams are focused on the use of data science, AI, and machine learning to develop more custom analytics. Also similar to larger organizations, improving alert and risk prioritization and operationalizing threat intelligence are seen as a priority. This includes a desire to improve processes and technologies for a more threat-informed defense.

Smaller teams are also focused on improving the integration of asset management data into the SOC as well as actively automating common security operations tasks.

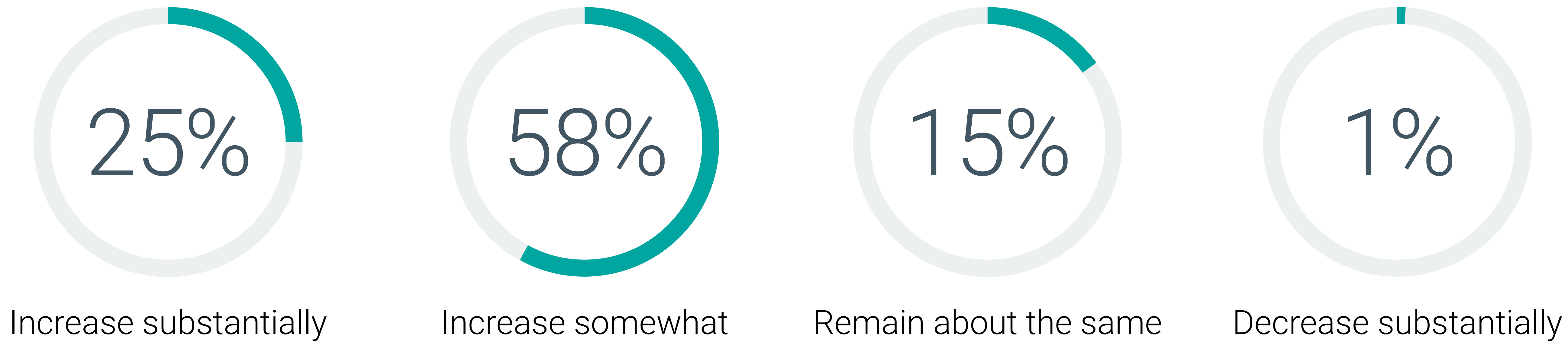
SOC-focused objectives organizations will pursue over the next 12 months.



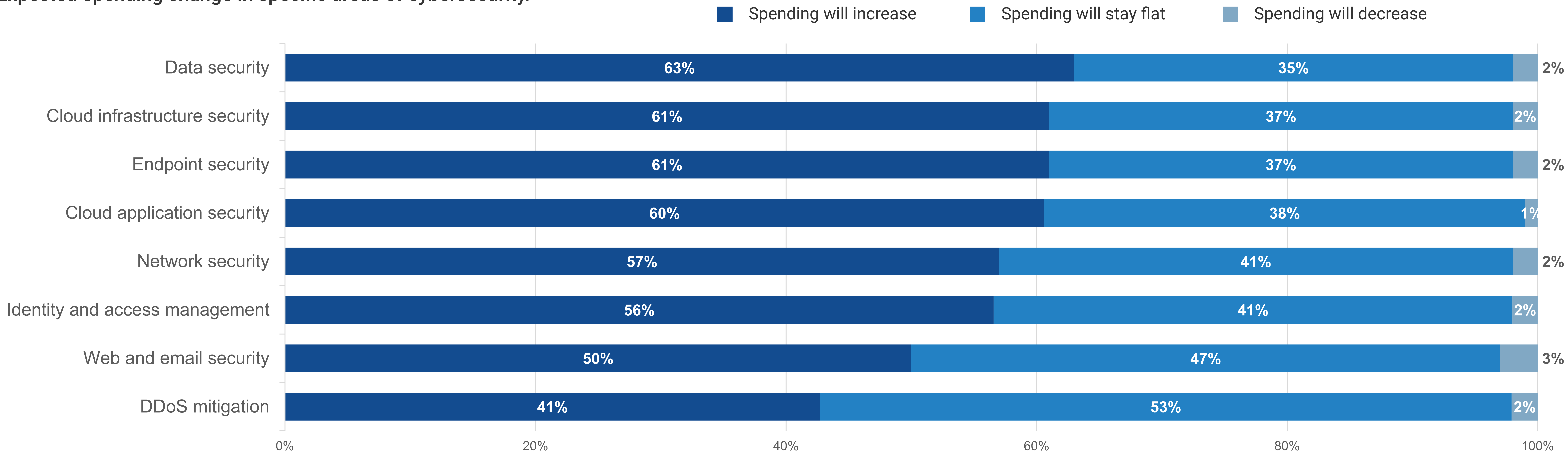
Most Expect to Increase Cybersecurity Spending Across Several Areas

The majority of organizations expect to increase their spending for cybersecurity operations technologies, services, and personnel relative to other areas of technology. While increased spending is planned to strengthen many facets of cybersecurity, at least six in ten organizations expect to invest more in data security, cloud security, and/or endpoint security.

Expected spending change for cybersecurity operations technologies, services, and personnel over the next 12 months.



Expected spending change in specific areas of cybersecurity.



CORO

ABOUT

Coro is leading the modular cybersecurity revolution. They are dedicated to making cybersecurity easy and accessible for small and mid-sized businesses.

Coro is on a mission to stop cyberattacks from hurting SMBs by offering an intuitive, affordable platform that allows businesses to focus on growth without worrying about security threats. They are working to build the most effortless cybersecurity solution available. Whether it’s a potential client, partner, or existing customer, Coro is committed to working together to protect and support businesses every step of the way.

Stop worrying about cybersecurity. Visit Coro.net today.

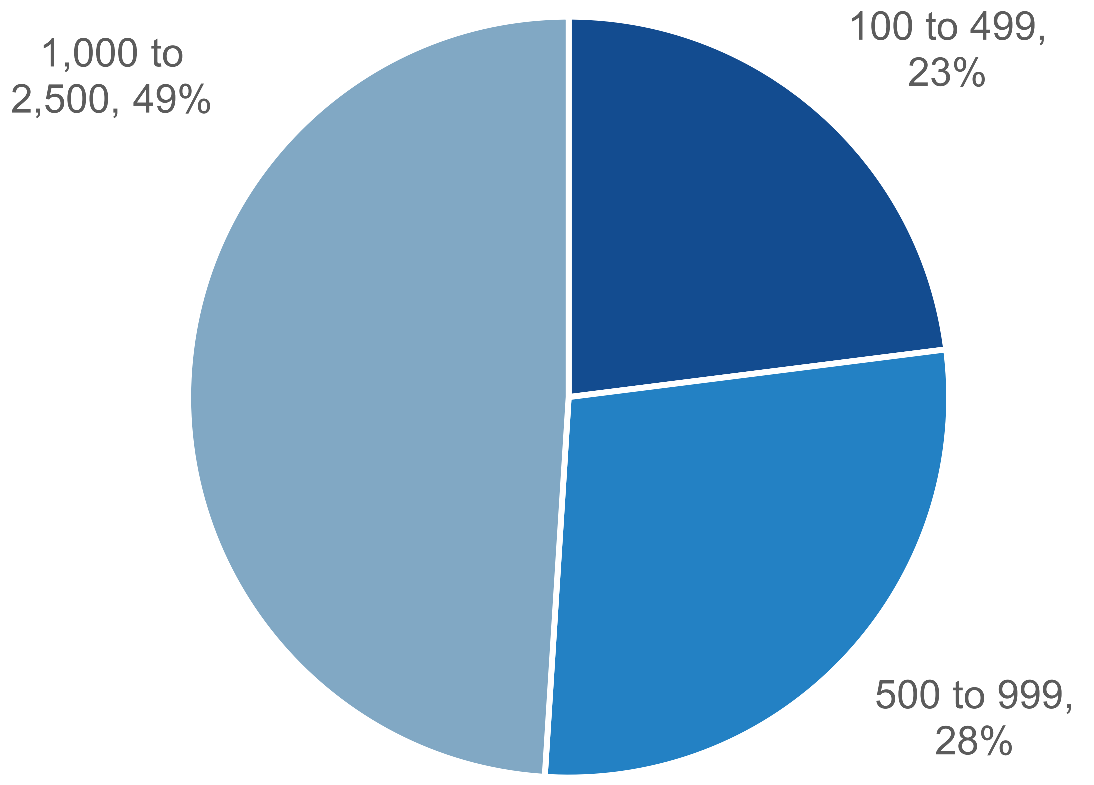
LEARN MORE

RESEARCH METHODOLOGY AND DEMOGRAPHICS

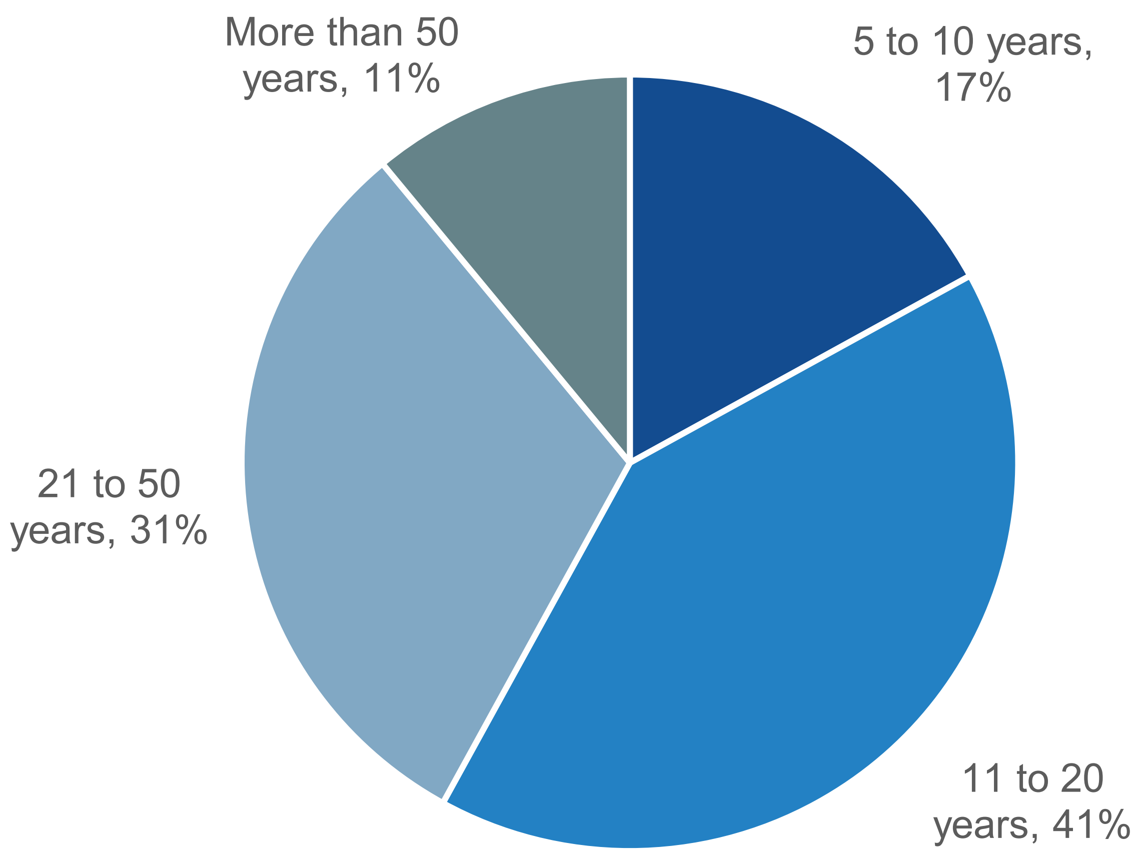
To gather data for this report, Enterprise Strategy Group conducted a comprehensive online survey of IT and cybersecurity professionals from private- and public-sector organizations across the globe between June 14, 2024 and July 11, 2024. To qualify for this survey, respondents were required to be involved with security technologies and processes at midmarket (i.e., 100 to 999 employees) and small enterprise (i.e., 1,000 to 2,500 employees) organizations. 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 379 IT and cybersecurity professionals.

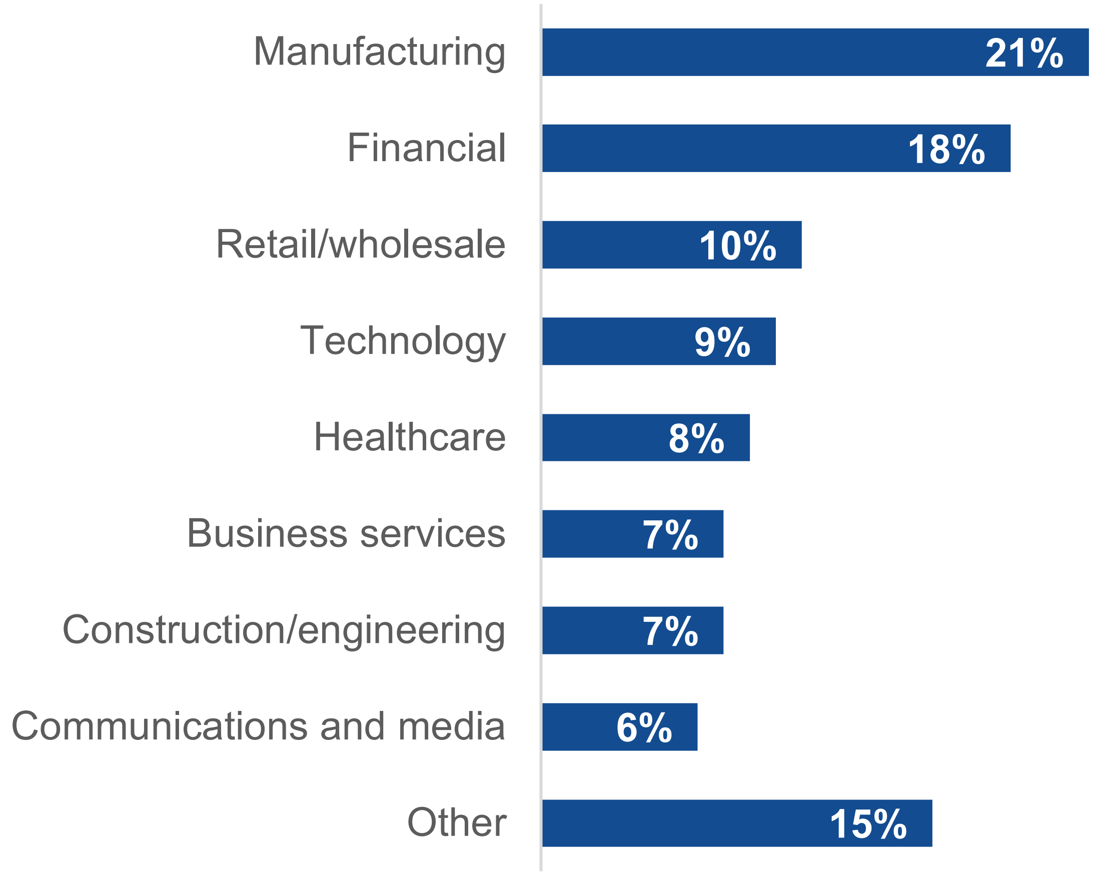
Respondents by number of employees.



Respondents by age of organization.



Respondents by industry.



Enterprise Strategy Group™ by TechTarget

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.