FORTRA

2025 Fortra State of Cybersecurity Survey Results

Index:

Introduction

Every year, we seek to see further by standing on the shoulders of giants — giants like you. The 2025 Fortra State of Cybersecurity Survey does just that.

Now in its second year, Fortra's State of Cybersecurity Survey canvasses expert opinions from practitioners around the globe regarding the trends that are likely to have the biggest impact on the year ahead. Drawing from the collective expertise of professionals from more than a dozen roles and over two dozen different industries, this year's State of Cybersecurity Survey reviews top issues like:

Risks and Challenges › Learn the year's top threats, how organizations are responding, and the challenges they are running into along the way.

Initiatives › From compliance to cloud to zero trust, see what security initiatives are top-of-mind in 2025 and why they might not be what they seem.

Tools and Vendors › Need is trending upward; tools are trending downward. See how teams are responding to increased supply, increased demand, and lower budgets.

Staffing › Despite the need to increase in-house skill levels, are organizations turning to more training? Or to something else?

As teams prepare to engage in another year-long battle with cybercrime, it is beneficial to examine where the industry sits in relation to the security issues that plague us all. We hope that the insights gleaned from this yearly report will help arm SOCs, CISOs, and other cybersecurity decision-makers with the perspective they need to guide their strategies over the next twelve months.

2025 FORTRA STATE OF CYBERSECURITY SURVEY RESULT HIGHLIGHTS

Each year, threat actors enhance their attack methods, compelling security professionals to adapt their strategies. We sought insights from industry experts about the upcoming year. Here are the key highlights we found particularly enlightening.

TOP INITIATIVES

77%
Identifying and Closing Security Gaps

75%
Improving Security Culture & Awareness

73%
Phishing/Malware

This year's top focus is on identifying threat vectors that need to be hardened. Improving security culture also continues to be a top focus as people are the first line of defense particularly when it comes to improving defenses for phishing and malware.

TOP EXECUTION CHALLENGES

59%
Budget Limitations

45%
Skills Gap

44%
Balancing Security and Business Efficiency

Security leaders always want to do more than what their budget allows, which includes improving skillsets of their staff or hiring for certain skills so they can enable the goals of the business.

TOP SECURITY FUNCTIONS TO OUTSOURCE

60%
Penetration Testing

56%
Email Security and Anti-Phishing

47%
Vulnerability Management

We continue to see an increase in managed security services adoption. The primary driver is to transfer a portion of operational burden to a third party to free up resources for higher value projects. This year there was a significant increase in outsourcing penetration testing to satisfy compliance requirements.

Risks & Challenges

TOP SECURITY RISKS

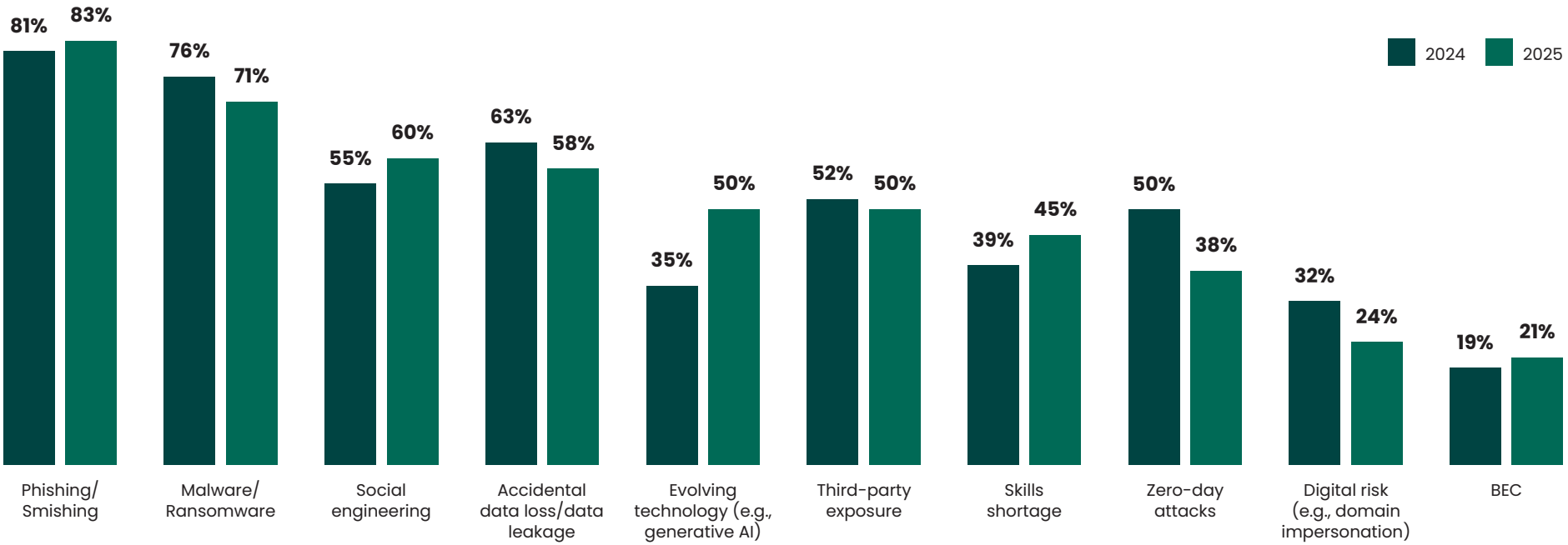
When asked to identify the top five most plaguing security concerns facing their organizations next year, respondents answered:

1. 83% | Phishing/Smishing (up from last year)
2. 71% | Malware/Ransomware
3. 60% | Social Engineering (up from last year)
4. 58% | Accidental Data Loss & Leakage
5. 50% | Evolving Technology (e.g., generative AI) (up 15% from last year)

Due to the explosion of sites, tools, and services leveraging emerging technologies like GenAI, the fact that one in two organizations consider "Evolving technology" one of the primary security threats of the coming twelve months is not surprising.

However, another phenomenon is zero-day attacks. Interestingly, the perceived risk of zero-day attacks dropped dramatically, falling from 50% in 2024 to 38% this year. This could be due to better detection and response tools in the market (and in security stacks) and the fact that so many of this year's AI-driven cyber tools claim to specialize in zero-day mitigation. While not in the top five list this year, another interesting trend was the increase in decision-makers worried about the potential lack of qualified workers, with "Skills shortage" increasing six percentage points, to 45%.

What are the top 5 security risks facing your organization in the next 6-12 months?



Risks & Challenges

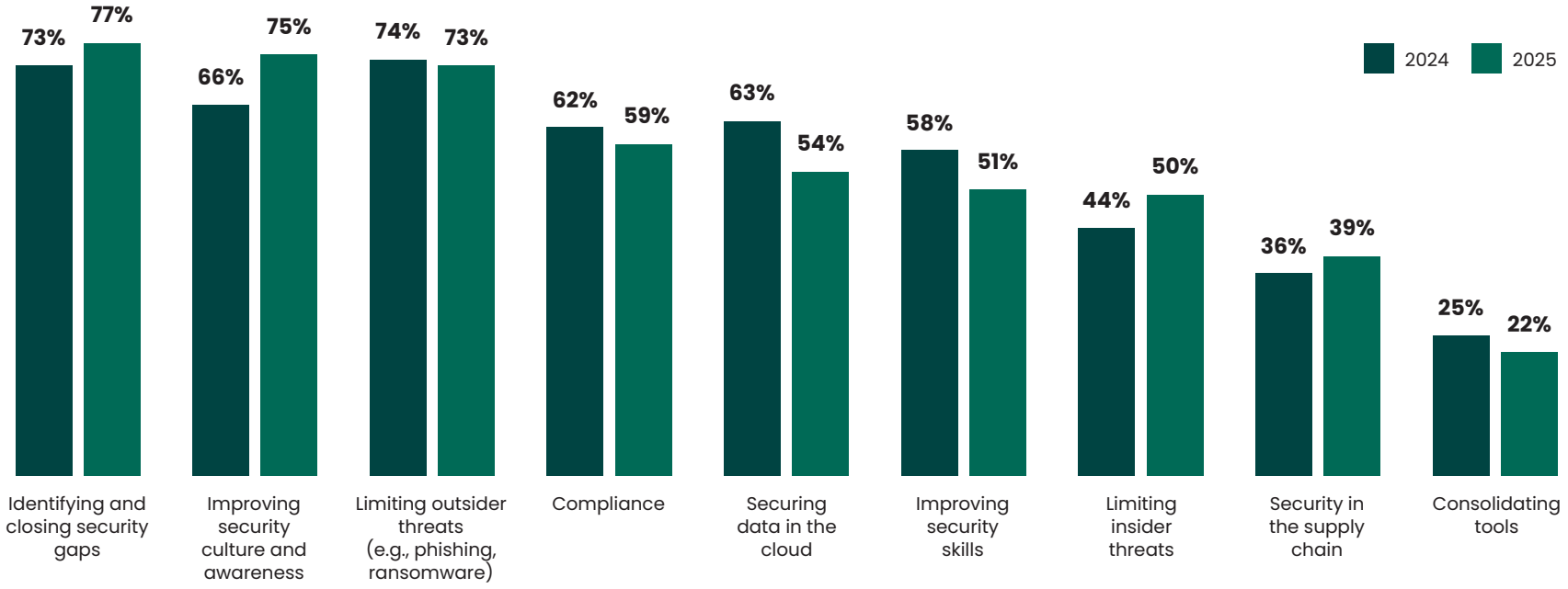
TOP CYBERSECURITY INITIATIVES

In light of the aforementioned threats, we wanted to see how organizations would translate their concern into security priorities in 2025. When asked what their organization's top five security initiatives were for the coming year, security experts responded that identifying and closing security gaps was first on their list (77%). It could be that companies are on the defensive as new forms of AI-based threats loom on the horizon and sprawling data feels exposed in an ever-growing cloud.

Notably, improving security awareness took the number two spot at 75% (up from 66% last year). It was encouraging to see a bump in these metrics, as teams know you can implement as many tools as you want, but your first line of defense is always your staff (especially in an era when social engineering sophistication is rapidly on the rise).

Also interesting was a dip in "Securing data in the cloud," dropping from 63% in 2024 to 54% this year, but that could be because cloud security is so ubiquitous now that it has ceased to be an "initiative" and has just been adopted into the "day to day." Also of note, despite the prescient desires to overcome the skills shortage and spot more security gaps, there seems to be a lackluster response when it comes to building up the needed security skills in-house. "Improving security skills" fell from being a priority for 58% last year to 51% this year, perhaps a sign that organizations want improvements made, but they might be more ready to wait and see if technology like AI (or an outsourced company) can make them first.

What are your organization's top 5 cybersecurity initiatives for the next 6-12 months?



Risks & Challenges

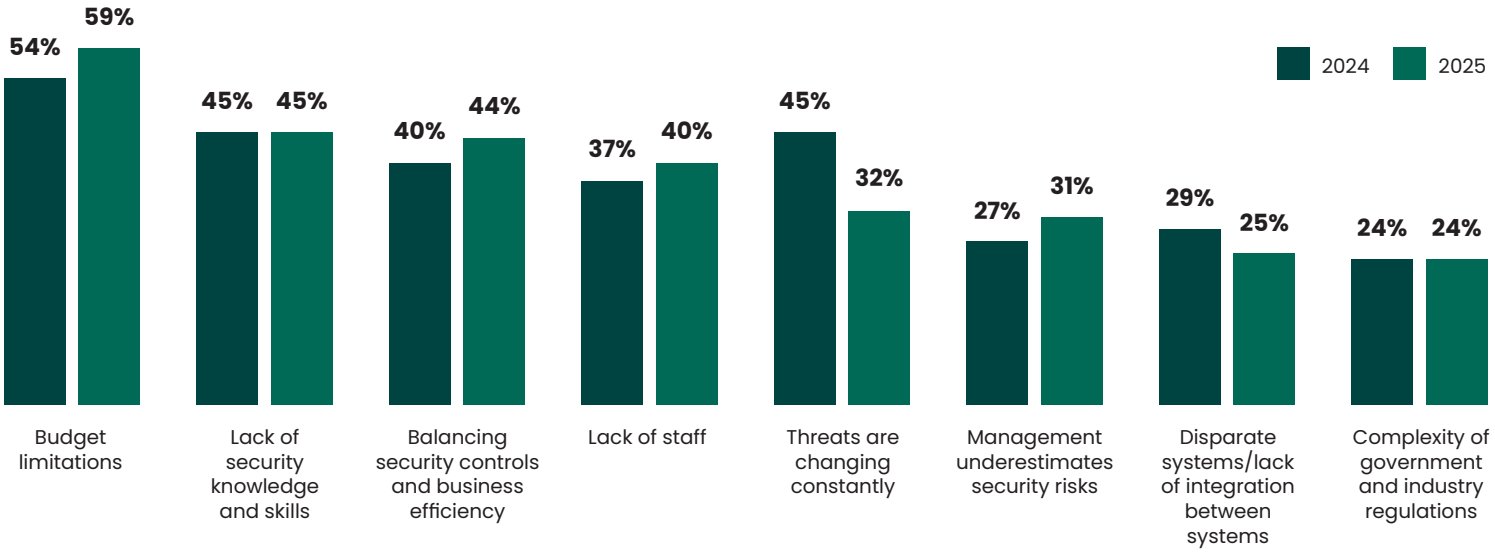
TOP CHALLENGES IN EXECUTING SECURITY STRATEGIES

For every plan, there is always a wrench. We asked respondents to postulate as to what that wrench might be in their own security plans for the coming year. A significant trend took shape, and not an unfamiliar one.

Budgetary constraints are always going to be at the top, and this year was no exception as 59% of respondents cited these as a top concern. As more boards, executives, and non-security C-suite members are being held accountable for cybersecurity debacles, the number of people allocated to secure — and some of the topmost jobs — is understandably being stretched to its utmost limits. Now, there are more than just the CISO and SOC with skin in the game.

Perhaps a bit surprisingly, constantly changing threats ("Threats are changing constantly") garnered only 32% of organization's top concern as a potential roadblock for upcoming security plans. This could be for the same reason cited above; constantly changing threats are no longer an exception but the rule. As such, dealing with them could be more a matter of course than a prioritized plan for most security teams. We certainly know it's not because of any deficit in evolving threats, and we largely have AI to thank for that.

What are the top 3 challenges you expect your organization to face when executing your security strategy in the next 6-12 months?



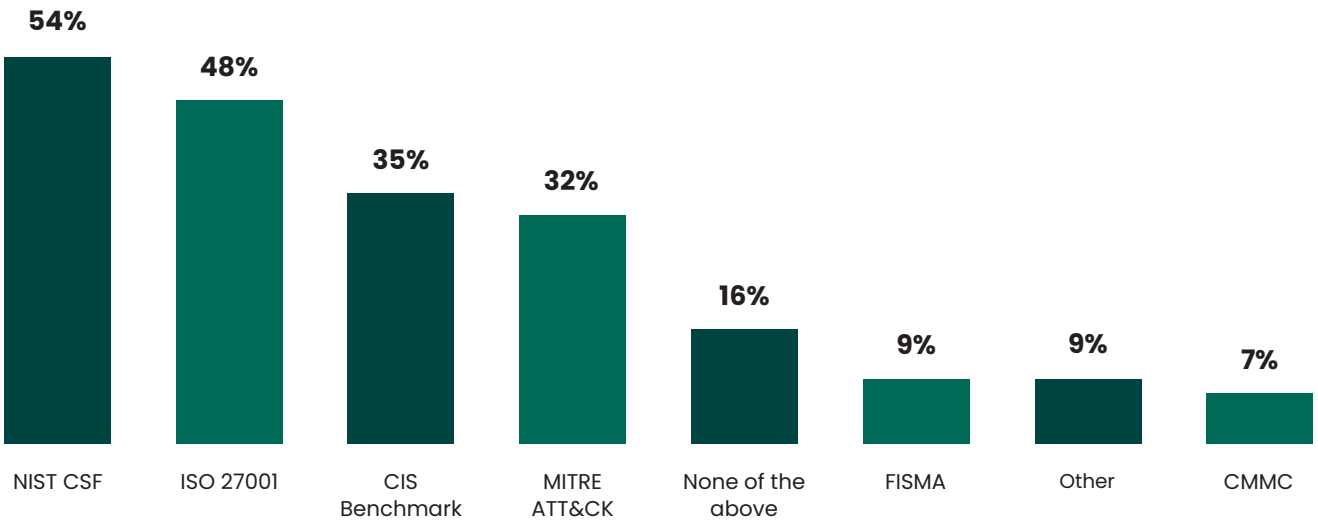
Initiatives

COMPLIANCE AND FRAMEWORKS

Despite the hype, even the most trusted and tried cybersecurity frameworks are only getting slightly over 50% use by most companies today. However, this isn't indicative of the value they bring to the table — only organizations' abilities (or desire) to implement them.

The NIST Cybersecurity Framework (CSF) saw the highest adoption rates at 54%, though still 5 percentage points down from last year. U.S. Department of Defense-specific CMMC unsurprisingly saw only 7%. However, the international standard ISO 27001 was almost as widely in use as NIST CSF, boasting a 48% followership, and MITRE ATT&CK took home slightly less than a third (32%).

Do you follow any of the below cybersecurity frameworks? Select all that apply.

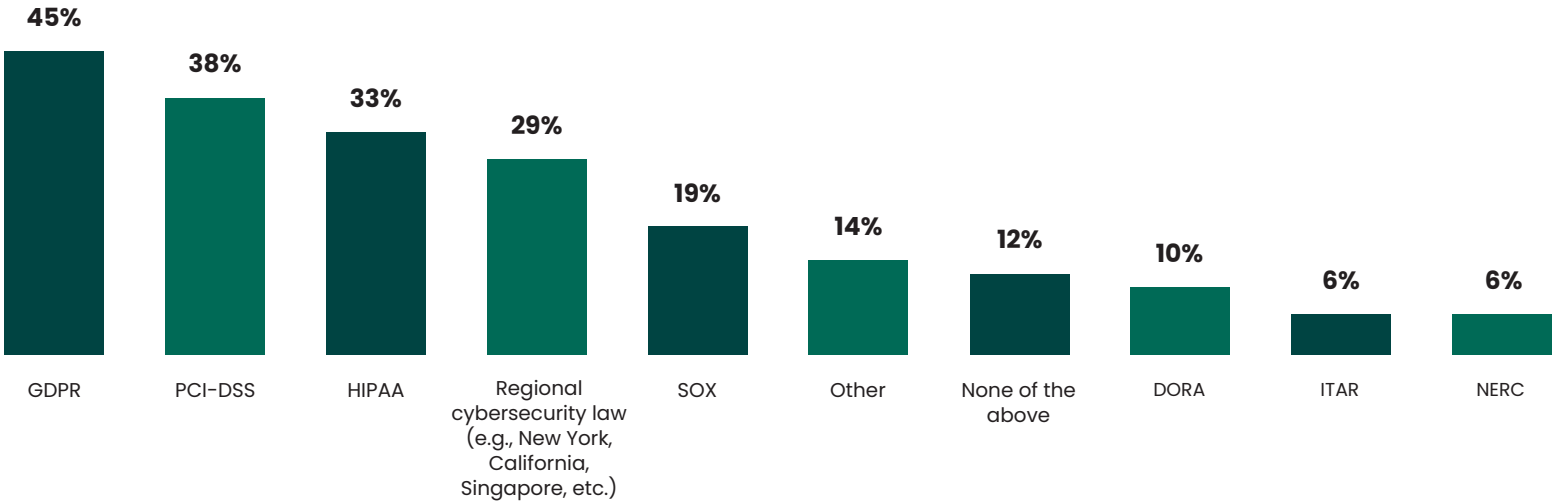


Initiatives

COMPLIANCE AND FRAMEWORKS

How are your compliance efforts going?

Which of the regulations below are you required to comply with? Select all that apply.



Initiatives

ZERO TRUST

When we get to the zero trust discussion, the responses read like a "nice but not necessarily necessary" assessment. That being said, nearly one in three (29%) has "already started implementing zero trust", and almost a quarter (24%) are even working with outside partners to build a zero trust roadmap for implementation.

However, just about the same amount (22%) noted that they were unprepared to move ahead with zero trust due to a lack of resources and skills, and 21% said the same, but due to operational complexities.

Zero trust gets a bad reputation sometimes as "a great framework, but hard to achieve." If you already have security best practices in place for other things, the issue becomes balancing newer and stronger zero trust provisions against the effort it will take to implement them. This goes back to budget limitations, and many are going to look to invest their money in something legally necessary (like compliance), no matter how useful zero trust is to those goals. Unfortunately, we may not see this change until zero trust becomes a necessary requirement in its own right.

How are you planning to implement zero trust across your extended environment?

Initiatives

CLOUD

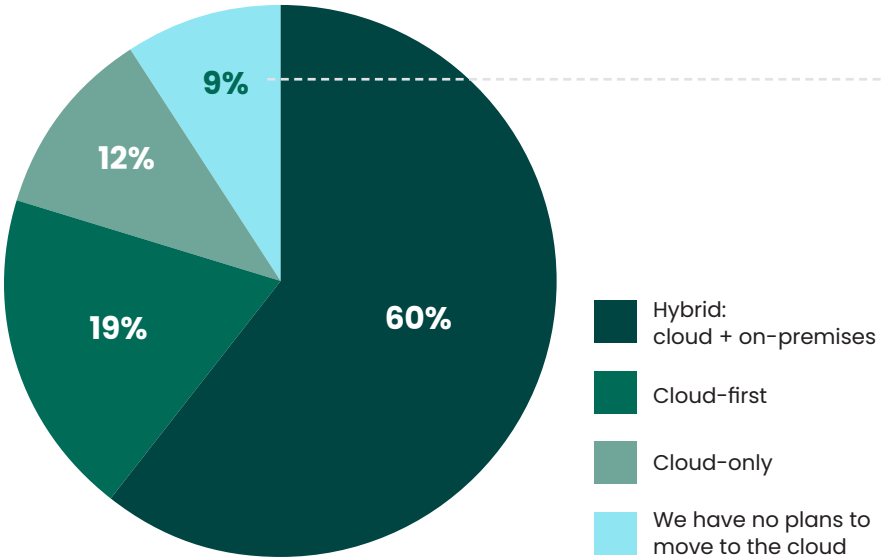
Six or seven years ago, companies started to lean into cloud-first models, prioritizing cloud-based solutions over traditional IT architectures. While forward-thinking, designing all new applications, platforms, and business structures to operate first — and best — in the cloud can require a lot of effort and clever ingenuity. Perhaps this is why only 19% reported doing it.

A cloud-only model is even more stringent, as organizations cannot rely on on-premises resources, even if doing so might make things easier. Additionally, it is expensive. Only 12% reported adopting this approach.

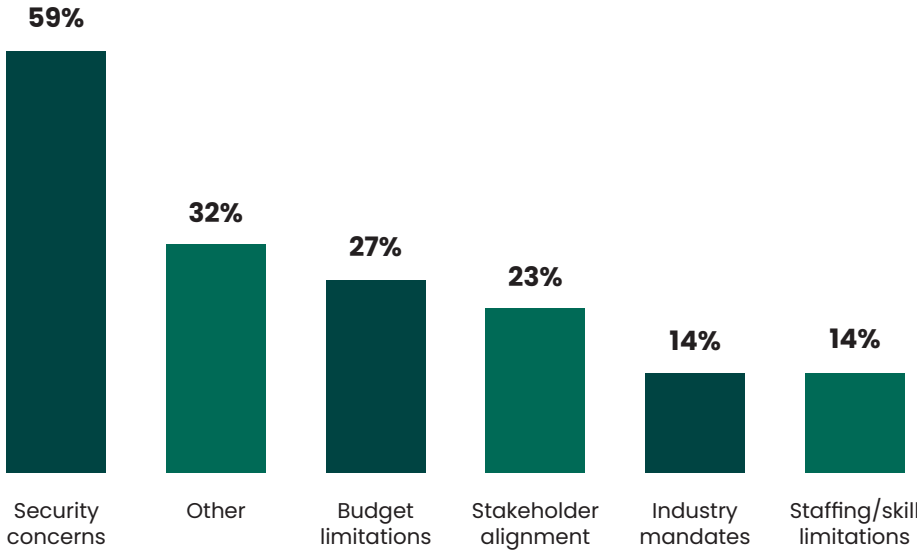
It becomes clear that cost — both in time and resources — is a huge factor in cloud adoption. The vast majority (60%) assume a hybrid model, which allows them to use either cloud or on-premises infrastructure when one or the other will work best. As cloud becomes the norm, everybody wants some of it — but not many can afford all.

Of those who decided not to move to the cloud (in any capacity), 27% did so out of budgetary constraints, 23% couldn't get stakeholder alignment, and 14% were constrained by industry requirements and staffing shortages, respectively. Interestingly, 59% chose not to due to security concerns (as one participant stated, "We are not sophisticated enough to understand what to do in the cloud"), but even this is on an upward trend as a full 77% avoided cloud due to security concerns last year.

Which best describes your cloud strategy?



How did your organization make the decision not to move to the cloud? Select all that apply.



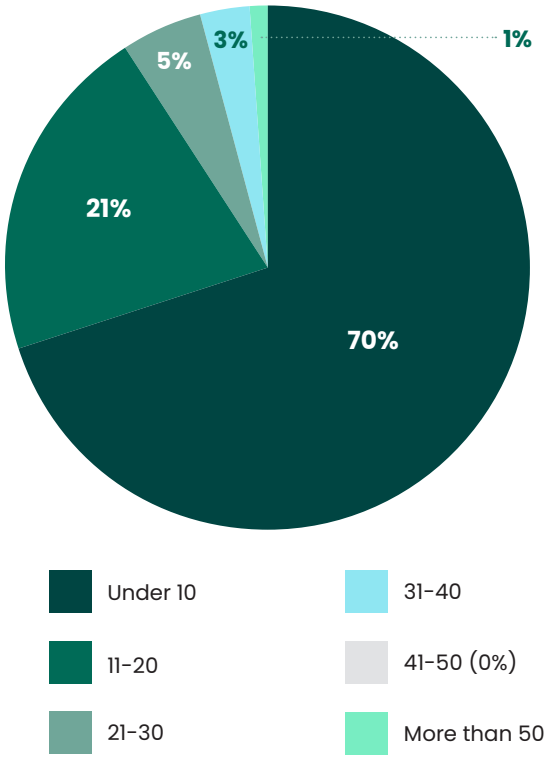
Tools & Vendors

CYBERSECURITY TOOLS AND VENDORS

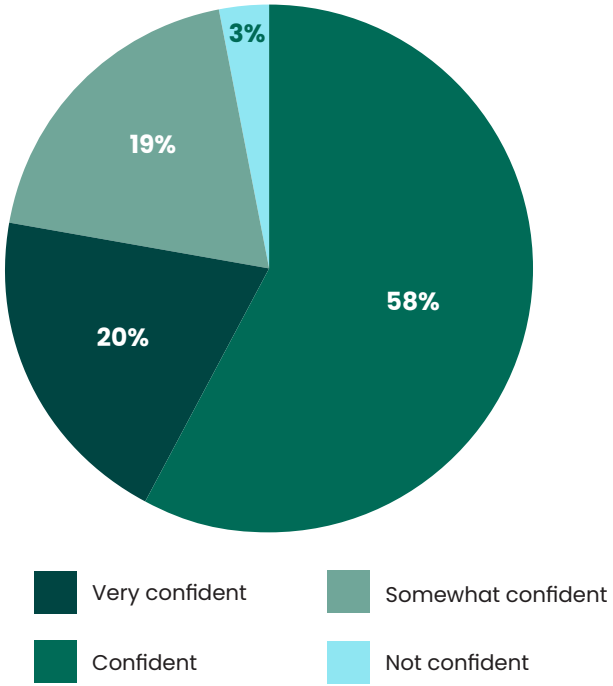
Speaking of security concerns, it seems that the vendor sprawl "boom" of the past decade or so might finally be ready to "bust." When asked how many security vendors they currently use, 70% answered that they use fewer than ten. This is a huge departure from the 60–75 vendors estimated in use by the average company even earlier last year.

When it comes to the tool stack nearly 1 in 4 said they were somewhat or not confident in their knowledge of what their security tools could do. Even these organizations find it difficult to prune their stack. Whenever companies change tools there is always a significant cost, both in implementation and in training. There can be an inhibiting concern about market volatility: Do we really want to change vendors right now, or should we play it safe? And ultimately, there needs to be a financial or notable business or security benefit to making the switch.

Approximately how many cybersecurity vendors do you have?



How confident are you in your knowledge of the security tools you deploy?

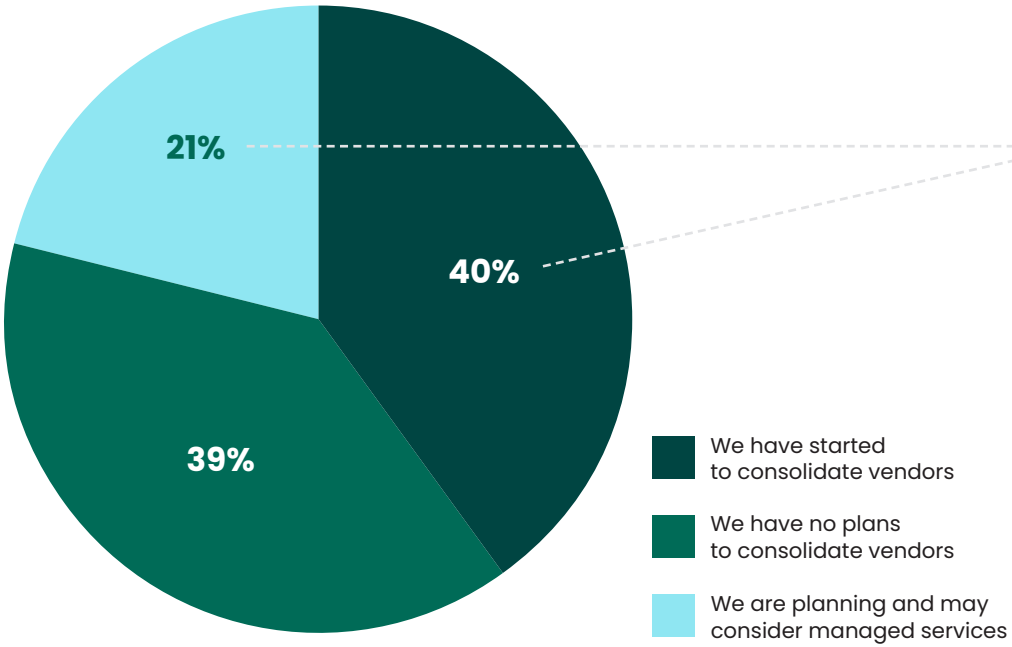


Tools & Vendors

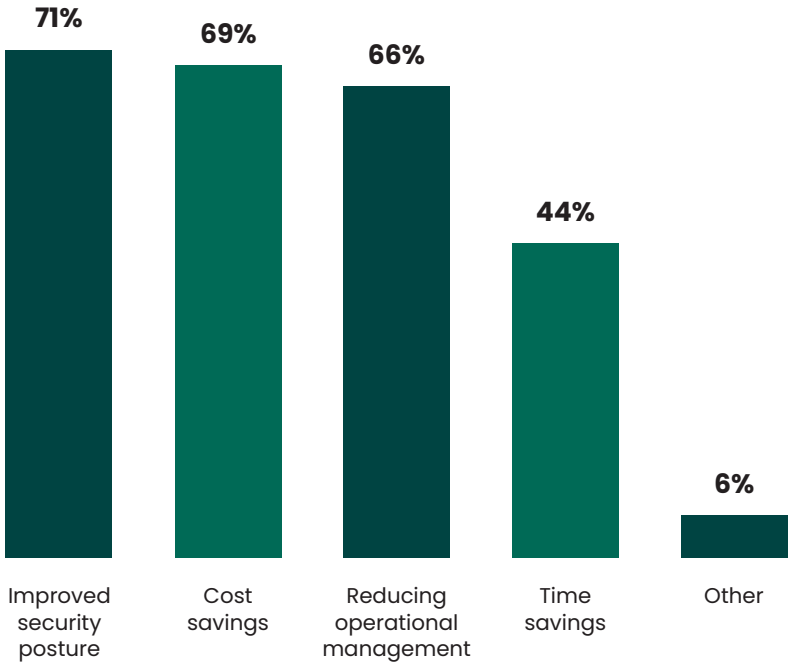
CYBERSECURITY TOOLS AND VENDORS

Notwithstanding, a full 61% expressed that they had already begun the process of vendor consolidation or were planning to start it, possibly leveraging the help of managed services. Another thing aiding vendor consolidation could be the fact that vendors themselves are taking on more tasks. Now, instead of offering single-solution products, more vendors are offering multiple features on a single product. This helps to eliminate unnecessary overhead and remove the management burden that comes with multiple tools and companies.

Where are you in your vendor consolidation journey?



What are your top drivers for vendor consolidation? Select all that apply.



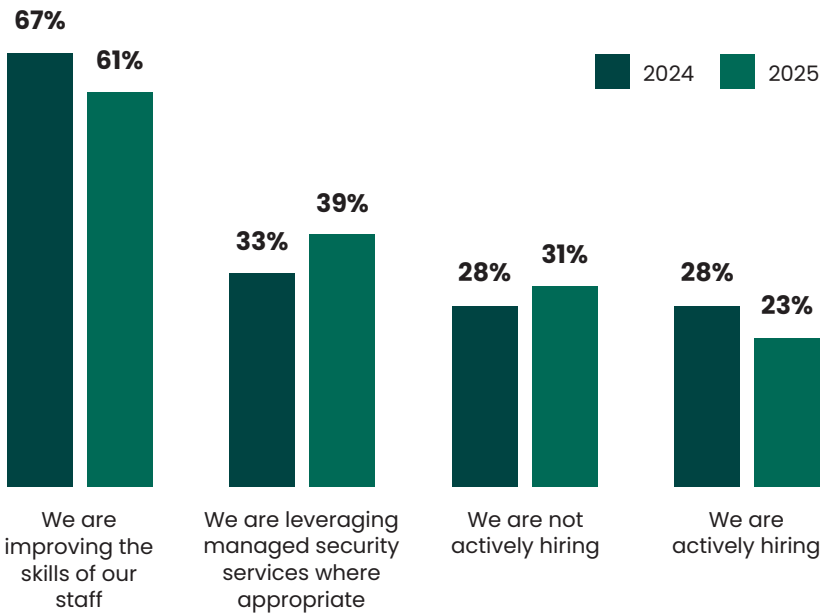
Staffing

STAFFING AND MANAGED SERVICES

As technology streaks ahead, companies are perhaps feeling the expertise burden of successfully managing complex cloud security, protecting hybrid environments, securing against AI-generated exploits, and navigating an ever-more complicated threat landscape. In the past year, the number of organizations "improving the skills of [their] staff" dropped (from 67% to 61%), while the number using managed security services has risen (from 33% to 39%). It is very probable that this trend might continue.

Given the problem of always trying to find (or train) enough experts, compounded by the breakneck pace of advancement, keeping SOCs constantly staffed with the skillsets needed to secure a rapidly changing digital world can be a task. If you take advantage of a third party that has the skills your organization lacks, you'll save costs on employees (hiring, training, etc.). Plus, with a more skilled security workforce, you increase your chances of saving any expenses you might otherwise risk in a breach.

What best describes your cybersecurity staffing strategy? Select all that apply.

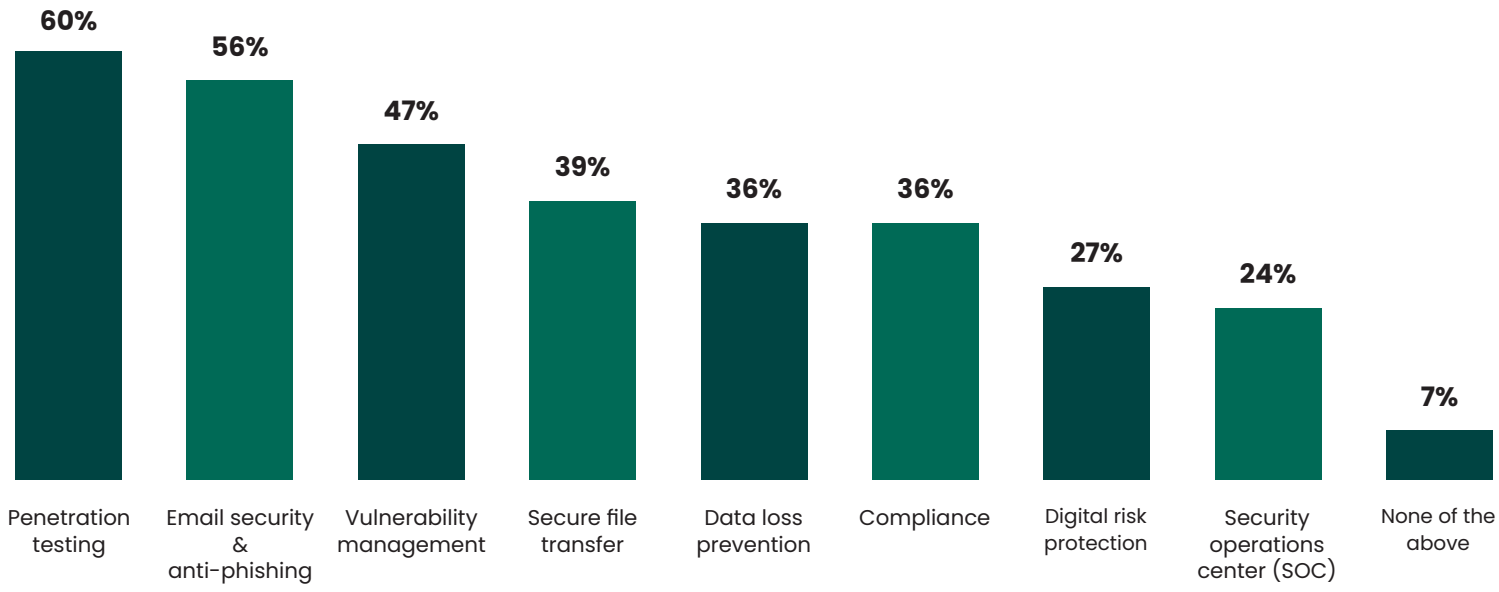


Staffing

STAFFING AND MANAGED SERVICES

Of those engaging in managed services, the majority (60%) used them for penetration testing services, followed by email security/anti-phishing (56%), and vulnerability management (47%). This is a notable trend as these solutions are proactive and preventative, rather than reactive and response oriented. It would denote a priority shift among defenders to stop breaches before they start, rather than investing solely in outside entities that could help with cleanup alone.

What cybersecurity functions do you currently engage managed services with (or if you're not currently, would you consider engaging)? Please select all that apply.



Demographics

INDUSTRY AND ORGANIZATION SIZE

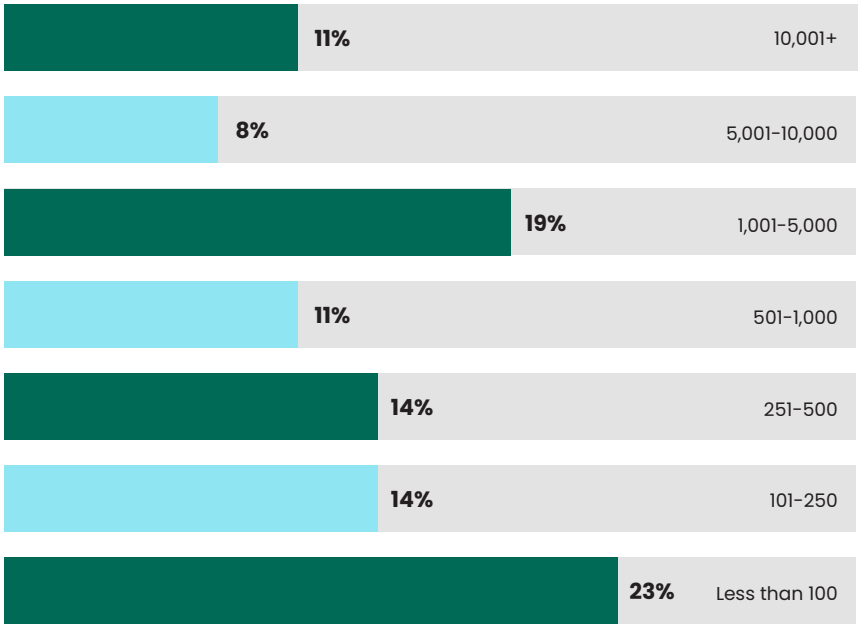
This year, our participants hailed from more than two dozen industries from Manufacturing and Retail, Cybersecurity, and more. The top five most represented sectors were:

1. Technology (16%)
2. Finance (15%)
3. Government (10%)
4. Manufacturing (9%)
5. Healthcare (8%)

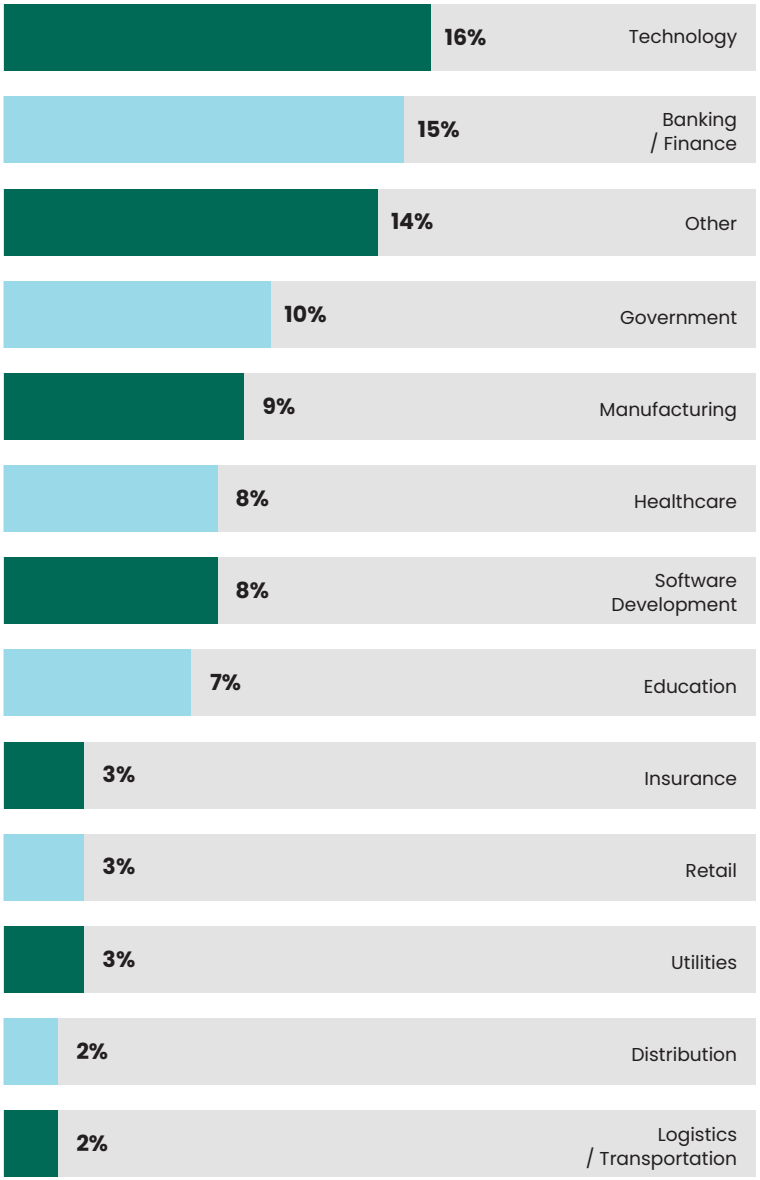
"Other" fields were written in by our respondents at survey time, which included Telecommunications, Mining, Hospitality, and others.

Organization sizes ranged from less than 100 employees (23%) to over ten thousand (11%). The second-most popular size bracket was companies containing over 1,000 up to 5,000 workers.

How many employees does your organization have?



What is your organization's primary industry?



Demographics

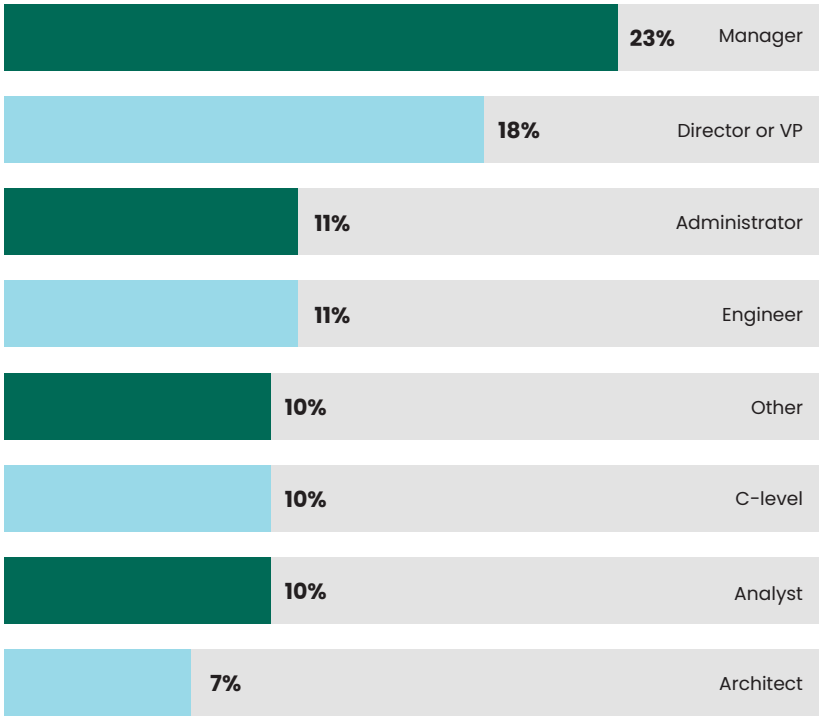
LOCATION AND JOB FUNCTION

In terms of the survey participants themselves, our respondents' job functions included:

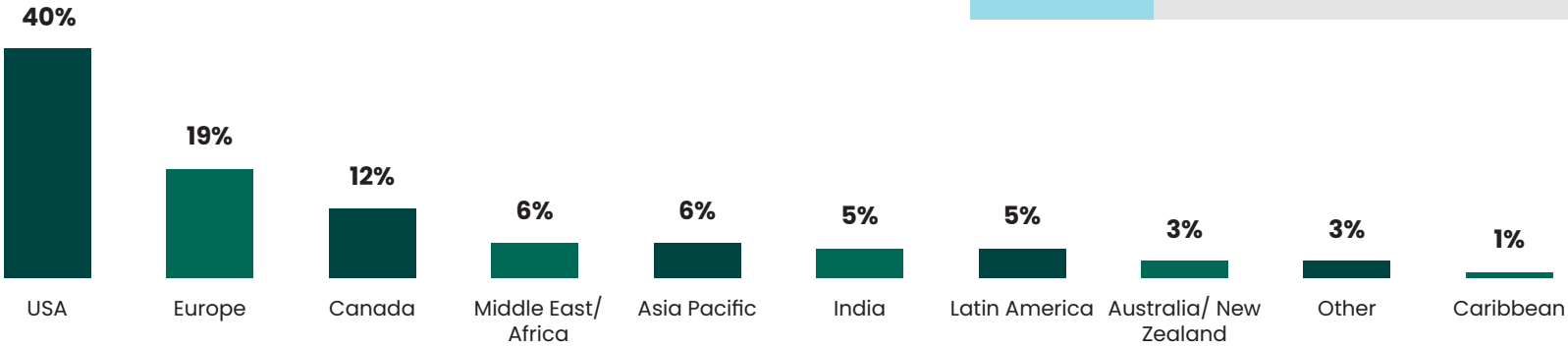
- Manager (23%)
- Director or VP (18%)
- Administrator (11%)
- Engineer (11%)
- C-Level (10%)
- Analyst (10%)
- Architect (7%)
- Other (10%)

Among the "Other" vocations were consultant, end-user support, SAP developer, Governance, Risk, and Compliance (GRC) coordinator, and Data Communication Channel (DCC) specialist.

What best descibes your job function?



Where are you located?



Closing Remarks

Cybercriminals are changing their tactics because we are changing our tactics and constantly getting better at what we do. Today's tools now catch more malware, zero days, and behavioral indicators than ever before, and threat actors are forced to hide where traditional tools can't reach. But even that is changing as organizations look to arm their employees with additional phishing and social engineering support, and "closing security gaps" rises to the year's top priority.

What We're Doing Well

Despite the year's challenges, there are a plethora of things the industry is doing well. The fact that things like cloud security and zero-day threats have decreased as urgent priorities is evidence that they are now being sewn-in as established parts of our security plans.

Organizations are doing what it takes to protect their assets in real time, hiring out when internal resources don't suffice and finding creative ways to get the job done. These are laudable accomplishments, and Fortra is proud to have been invited to contribute to these successes in any way.

The problems have been insightfully identified, and organizations are already taking steps to solve them. We've seen an increase in proactive measures like penetration testing, and a desire to protect-at-all-costs by leaning on managed services to address resource shortages when necessary.

Keeping Attackers on the Defensive

Going forward, it is important to continue to nail the fundamentals. Threat actors will always try to capitalize on obvious security measures we have missed, especially as we make things harder for them everywhere else.

To stay one step ahead, identify opportunities for automation (i.e., those repetitive tasks) because attackers do. They have no qualms using AI, automated techniques, and the as-a-Service underground economy for their gain, and to keep up, we need to force-multiply our SOCs with as much autonomous help as possible.

And lastly, supplement your tools with managed services as needed to get a handle on the new technologies, new techniques, and new threats out there. This transfers a portion of your operational burden to a partner and frees up your resources to work on higher value projects.

Close the Gaps with Fortra

As we move into 2025, Fortra is excited to stay online and in the trenches with organizations like yours. The challenges you face directly impact the solutions we create, and your generous feedback in surveys like this enables us to keep moving you forward. Together, we can continue to force attackers to change their moves as we learn about them, analyze them, and fight them in the year ahead.

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.

fta-gd-0125-vm