FORTRA™

2024 Fortra State of Cybersecurity Survey Results

Index:

Introduction

Tomorrow's changes come from today's problems. At Fortra, we believe that our customers have the sharpest perspective on what's going on in the industry, being as they are on the front lines of today's real-world security challenges. We wanted to put these invaluable customer insights to good use by capturing them in a yearly survey that will add to the knowledge base of the cybersecurity community at large.

To that end, we are proud to present the results of our inaugural 2024 Fortra State of Cybersecurity Survey. For this report, we canvassed opinions from over 400 security professionals within 40 different industries across the U.S., Europe, Canada, Asia, the Middle East, Latin America, the Caribbean, Australia, and New Zealand.

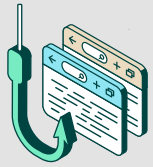
Their responses were candid and insightful, and we express our appreciation for their authentic contributions. We know their feedback will guide our strategy in the coming year, and we hope you find their insights as valuable as we did.

Our respondents were asked to open up about the challenges they've faced while securing their digital enterprises over the past year. We are at a critical juncture in digital transformation. The distributed workforce is now the norm, and companies must support remote productivity of which cloud will play a key role. This requires leaders to plan security for hybrid infrastructure – a distinct departure from the inherited on-premises strategies of most organizations. That's why there is a lot to learn from this year's temperature check on the industry.

2024 FORTRA STATE OF CYBERSECURITY SURVEY RESULT HIGHLIGHTS

Every year the threat actors improve their attack campaigns requiring security professionals to evolve their strategies. We were interested in hearing what our customers and partners had to say about the upcoming year. Here are the highlights we found insightful.

TOP INITIATIVES FOR 2024



74%
Phishing/Malware

73%
Identifying and Closing Security Gaps

66%
Improving Security Culture

"The top focus is on improving controls and processes around phishing and malware followed by identifying the latest attack vectors for hardening. Security leaders know that improving security awareness has a direct correlation to improving phishing and malware defenses, so they have made improving security culture a top initiative as well. Improving security culture should also free up resources so they can focus on cloud security as organizations continue to adopt cloud-first and cloud-preferred strategies."

-**Antonio Sanchez**,
Principal Cybersecurity Evangelist

TOP EXECUTION CHALLENGES

54%
Budget Limitations

45%
Constantly Changing Threats

45%
Skills Gap

"Budget limitations coupled with the constantly changing threat landscape are two of the top executional challenges for professionals responsible for the security posture of an organization. The skills gap is also a top challenge as analysts are required to be experts in multiple security domains as well as cloud."

-**Wade Barisoff**,
Director of Product, Data Protection

TOP SECURITY FUNCTIONS TO OUTSOURCE

58%
Email Security /Anti-Phishing

52%
Vulnerability Management

51%
Data Protection

"Burnout is one trend that's causing skilled people to leave organizations or transition into roles with more targeted responsibilities. This puts additional stress on the remaining staff as they must still deliver the required outcomes with fewer headcount. We are seeing increased adoption in managed security services to relieve a portion of their operational burden."

-**Josh Davies**,
Principal Technical Manager

Risks & Challenges

TOP SECURITY RISKS

Looking forward, most organizations anticipate phishing (81%), malware and ransomware (76%), and accidental data loss (63%) will be the top security risks over the next six months, followed by social engineering (55%) and third-party risks (52%).

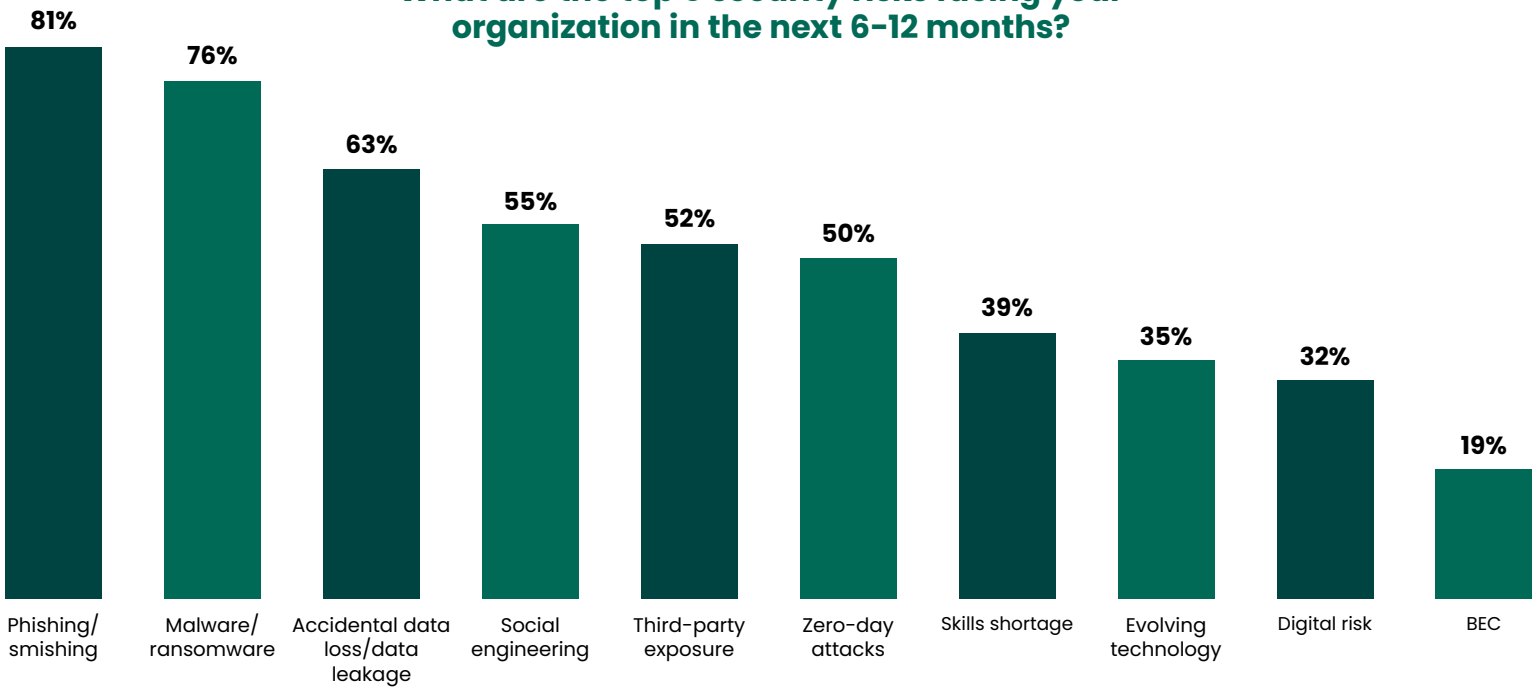
This seems about right for the threat landscape we're facing, though our analysts note changes that could be contributing to these figures. Although not a record year, the number of reported zero-day exploits seen in the wild was high. Zero-day exploits take longer to detect, giving attackers a longer window of compromise, contributing to ransomware fears. There are additional contributing factors: a larger attack surface, increased financial interest, the recent resurgence of espionage malware, and more third-party brokers as supply chains expand.

A recent scare tactic that could be boosting interest in ransomware is that of attackers threatening to report breaches to the Security and Exchange Commission (SEC), adding injury to insult. These attackers compromise the network, breach critical data, then, in addition to demanding a ransom, threaten to notify authorities of the victim company's faulty security posture if the ransom is not paid.

The advent of AI-generated phishing emails makes it possible for convincing fakes to be sent with minimal effort, including to countries that were typically protected from high phishing rates before, due to complex alphabets and language difficulties.

Email phishing is still the go-to attack used to target your workforce and supply chain. Get advanced threat protection from an integrated cloud email security platform. Discover Fortra's Cloud Email Protection ›

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



Risks & Challenges

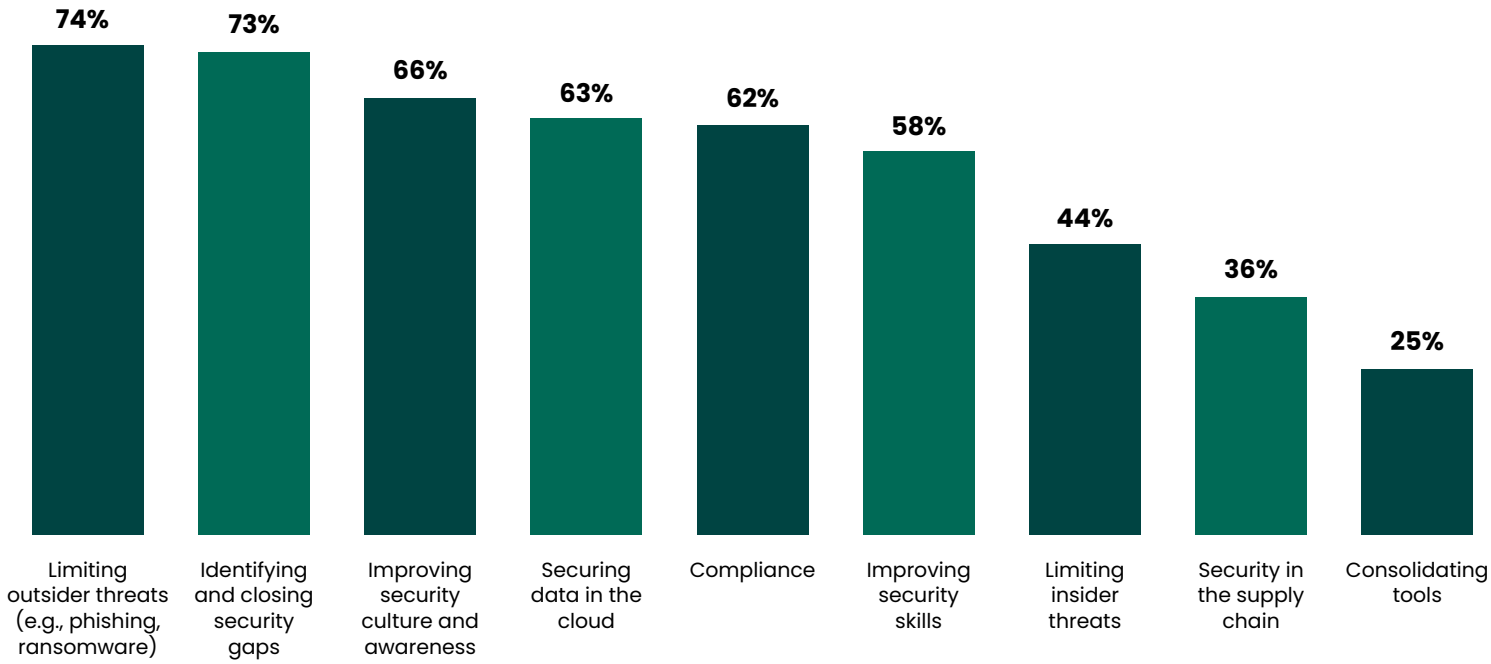
TOP CYBERSECURITY INITIATIVES

Most survey participants stated that their top five cybersecurity initiatives for the following year include limiting outsider threats (like phishing and malware) (74%), finding and closing security gaps (73%), improving security culture (66%), securing the cloud (63%), and compliance (62%).

While these seem like disparate tasks, many stem from the same source – the headlong rush to the cloud, the consequences of which came home to roost in 2023 and will still be playing out this year. In the frenzy to go digital during the pandemic, rush jobs were the order of the day, and weak policies, poor container security, misconfigurations, and gaping security holes were the result. Now, companies are trying to pick up the pieces. Any one of the above problems can be likely traced back to rapid cloud migration, and only properly deployed cloud security can be the rising tide that lifts all ships. Because today, most ships are sailing in the cloud.

Reducing your risk begins by continuously identifying and closing your security gaps, wherever they're hosted. Discover Fortra solutions for vulnerability management ›

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



Risks & Challenges

TOP CHALLENGES IN EXECUTING SECURITY STRATEGIES

When asked to identify the top three things standing in their way, respondents cited budget limitations (54%), the constantly changing nature of threats (45%), and lack of security skills (45%) as the top three impediments.

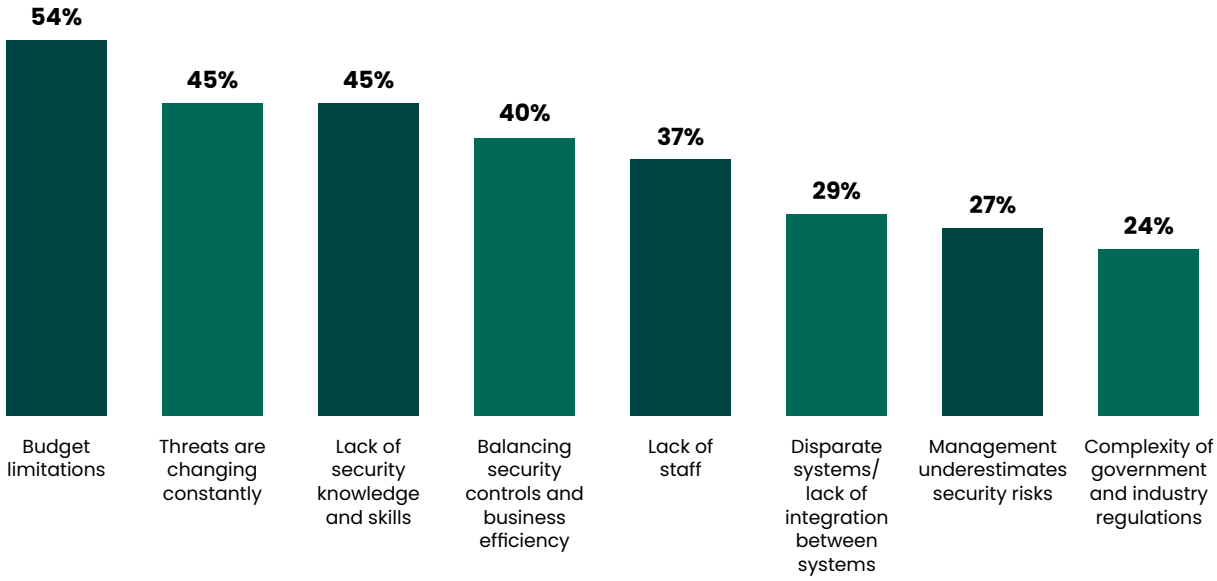
These three challenges, along with others mentioned, have contributed to the creation of a very transient cybersecurity culture. "Not enough to do the job" means everyone has to wear many hats. Consequently, no one is an expert. Ten years ago, you might have seen specialists in malware, data loss prevention, or some other security niche, but increasingly, environmental security forces have made siloing expertise ever more of a luxury.

Additionally, our analysts add a word of caution about the way companies may go about remediating these issues. It may be tempting, especially as features, capabilities, and promises improve, to jump headlong into artificial intelligence (AI) like we did with the cloud. But we know how that went. The problem here is not so much misconfiguration, but the fact that the AI landscape is still very much the Wild West, and early days in terms of security standardizations, development guidelines, and protective legislation. The requirement for accuracy in defensive security tasks is high, so AI should be used to augment security functions rather than take them over entirely. Engage at your own risk.

On the bright side, our analysts noted increasing C-level engagement in cybersecurity initiatives as a potential counterbalance to some of these obstacles.

Keep pace with the ever-changing threat landscape. Fortra's multi-vector approach to threat research works tirelessly, so you don't have to.
Discover Fortra Threat Brain ›

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



Initiatives

ZERO TRUST

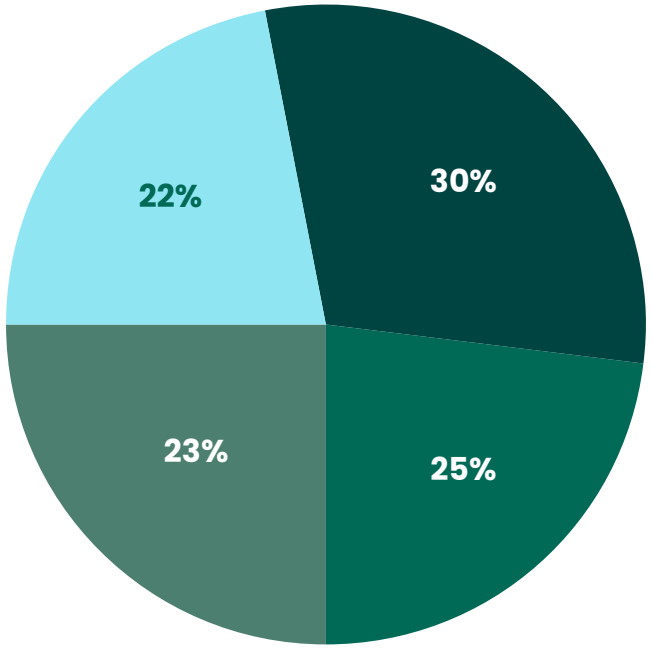
Everyone is seeking to implement principles of zero trust (ZT), especially as the expanding digital landscape leaves so many holes where inherent trust slips in. Every new integration requires raking over with a fine-toothed comb to make sure no new holes are introduced. When asked how they planned on implementing ZT across their extended environments, 30% answered that they were partnering with multiple security providers to get it done. A quarter said they weren't planning on it due to insufficient resources, and 23% simply responded that they'd already started.

Achieving zero trust within a hyperconnected environment is a never-ending endeavor which will never be fully achieved. However, to strive for anything less would be to knowingly leave holes open where there shouldn't be and give up the only security fight worth fighting: ultimate protection of your enterprise across the digital realm. A reasonable way to look at it now, however, is to prioritize your zero trust dominoes and knock them down, one by one, based on criticality.

Seek ZT for your most essential assets, then your second-most, and then go from there. That way you can strategically introduce the most protection while still in progress towards your goal.

Fortra serves as an ally and partner in the process, helping first identify the problems you need to solve and then determining what controls will fit your problem set. Discover Fortra support for zero trust ›

How are you planning to implement Zero Trust across your extended environment?



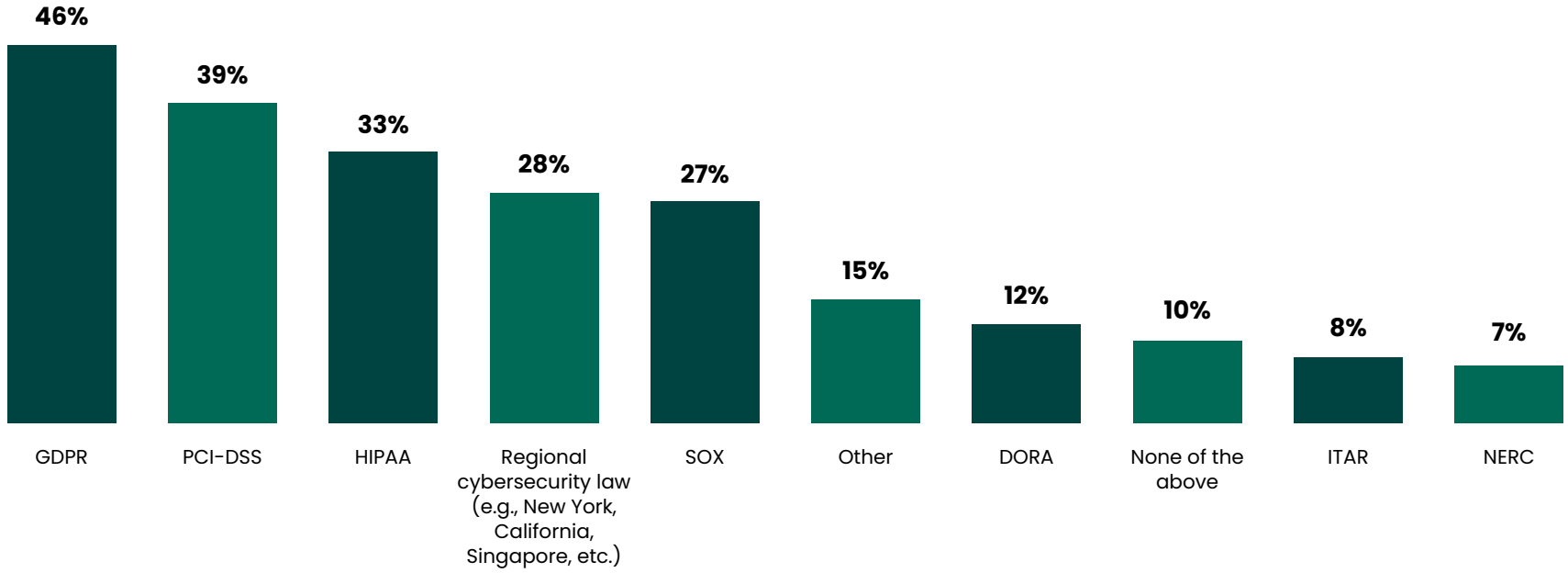
Initiatives

COMPLIANCE AND FRAMEWORKS

Most respondents were required to adhere to GDPR (46%), PCI-DSS (39%), and HIPAA (33%), followed by regional cybersecurity laws (28%), and SOX (27%). What we're seeing now is a lot of overlap, as organizations are facing multiple requirements from different sectors of compliance. A California-based healthcare company, for instance, could be subject to HIPAA, PCI-DSS, CCPR, and GDPR (if they choose to offer international telehealth services).

While this may introduce some challenges, companies are widely optimistic. 63% reported feeling confident; "we know how to get there." 28% felt good but needed some help, and 9% needed the help (without feeling good). Most adhere to some type of cybersecurity framework, with NIST (59%), MITRE ATT&CK (44%), and CIS Benchmark (36%) being the top three.

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



Initiatives

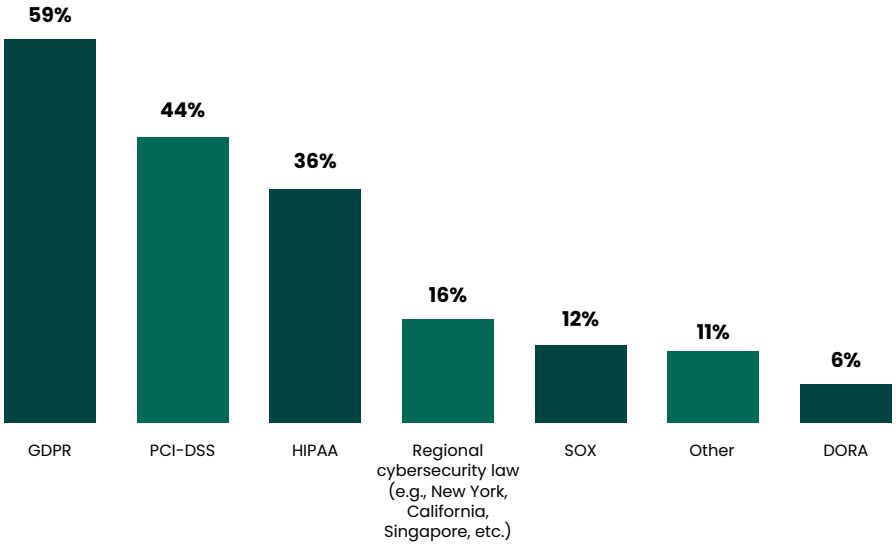
COMPLIANCE AND FRAMEWORKS

The clarity and re-clarification of frameworks that we've seen since their inception have likely played a role in companies feeling so confident, and this is a good thing. NIST adoption is no surprise, as it is widely seen to be the best one at demonstrating areas of protection.

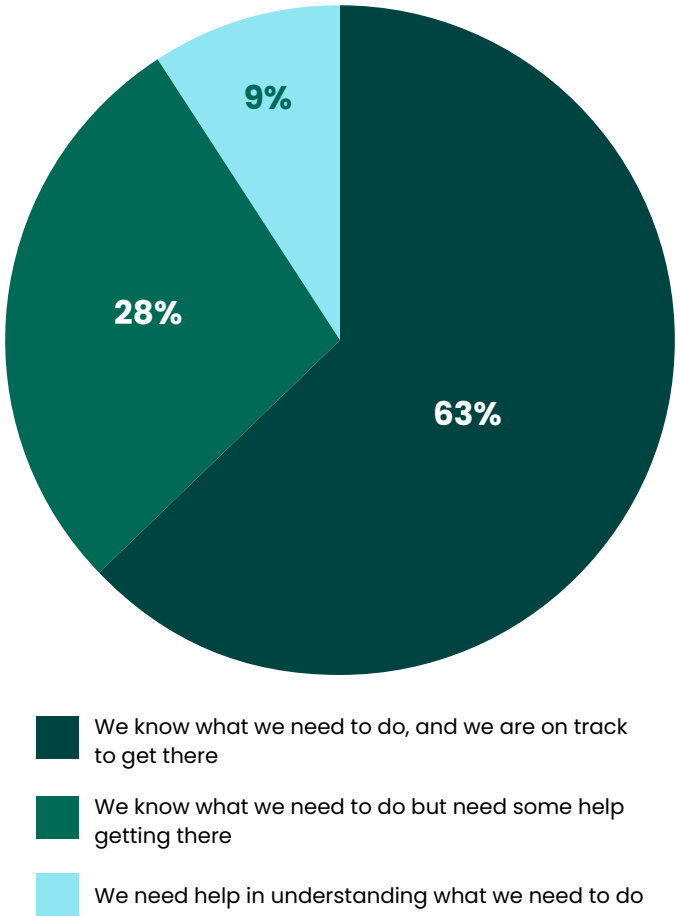
Interestingly, frameworks relating to supply chain security didn't feature as highly as might have been expected, given the 36% interest in making it a "Top 5" priority for the coming 6-12 months. This may be because supply-chain centered legislations such as DORA and CMMC 2.0 are over a year out and there is low representation of the organizations that would be affected.

Ace your next audit with Fortra and take the guesswork out of the compliance process. Discover Fortra support for compliance and frameworks ›

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



How are your compliance efforts going?



Initiatives

CLOUD

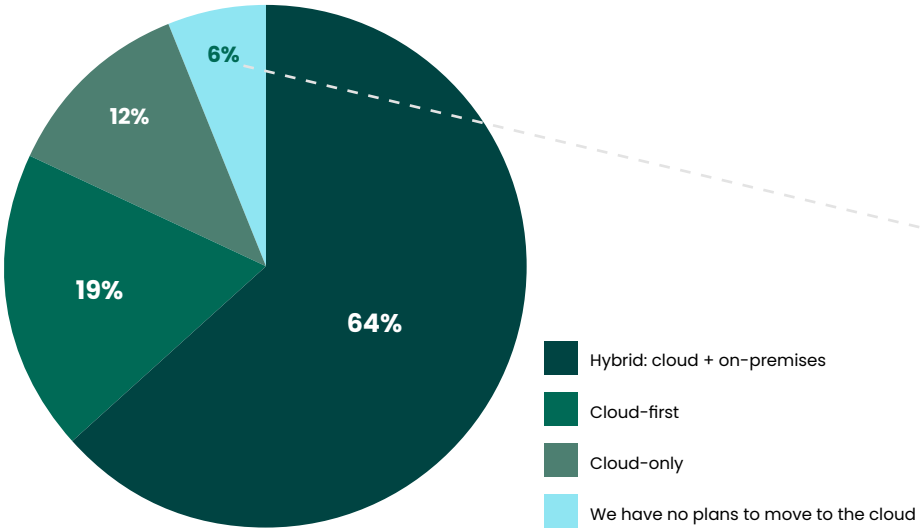
The vast majority of respondents reported having a hybrid environment (64%), while 19% were cloud-first, 12% were cloud-only, and 6% had "no plans to move to the cloud." The strong turnout for hybrid is consistent with what we hear in markets with high cloud adoption. In these regions, organizations are adopting a cloud-first or cloud-preferred strategy, but still need to keep an on-premises presence for things like compliance and privacy mandates. Other reasons for the lingering footprint include custom-built legacy applications that provide critical functions and risk diversification (i.e., placing your eggs in multiple baskets so that operational interruption in one environment does not bring business to a complete halt).

When asked why their organizations decided not to make the jump, those 6% cited security concerns (77%). This was higher than we initially expected. Following that was stakeholder alignment (or lack thereof) (35%), industry mandates (common in critical infrastructure) (31%), and staffing and skills limitations (31%). Interestingly, budget restrictions only accounted for 19% of non-adopters.

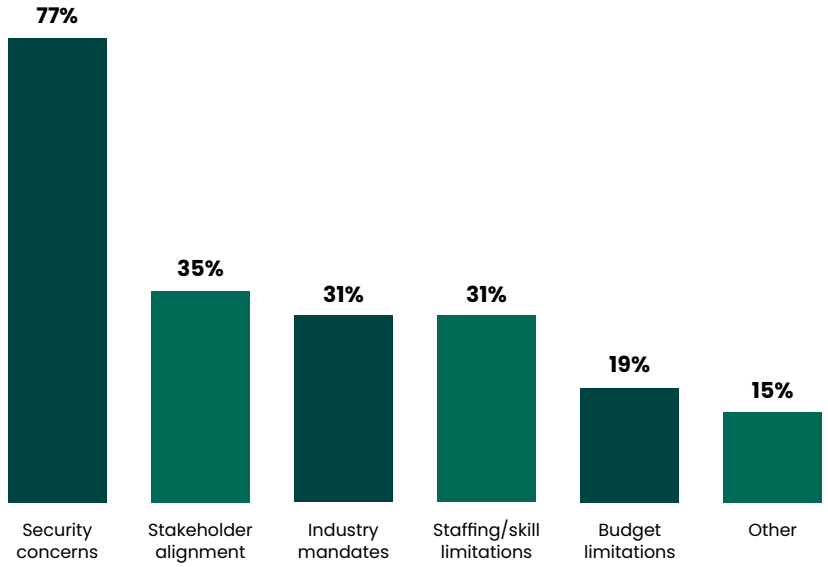
This is a very understandable place to be, and in many ways, a wise one. Critical industries that support the national economy and protect national security need to be sure that their migrations will be effective, secure, and minimal in downtime. Sectors like energy, water, and nuclear development don't have the luxury of rush adoption, only to get it wrong. In fact, NERC-CIP (the regulatory backbone of the U.S. electric grid) doesn't allow cloud usage at all.

For those who are active in the cloud, Amazon Web Services (AWS) is a popular choice. While AWS provides you with tools to protect your AWS environment, it is still your responsibility to correctly deploy and maintain those security services across your AWS accounts and applications. Discover Fortra support for AWS ›

Which best describes your cloud strategy?



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



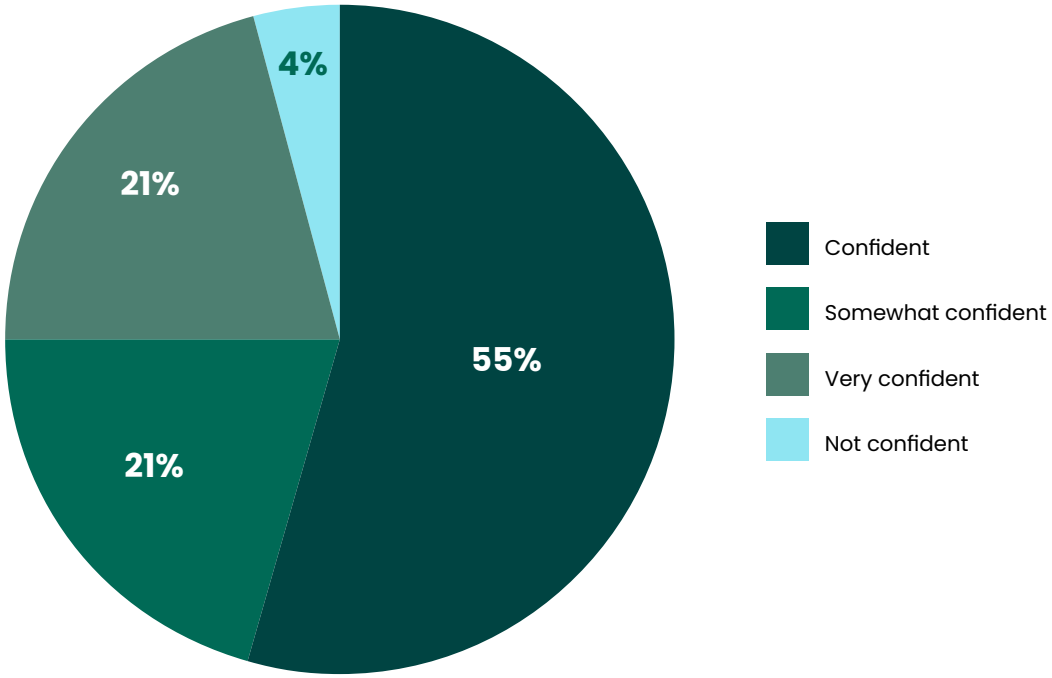
Tools & Vendors

CYBERSECURITY TOOLS AND VENDORS

Reducing tool and vendor sprawl has been another widely discussed topic within the security community, especially as many companies see their investments turning into shelfware. Initially intended to unburden teams, the compatibility factor, time it takes to learn, and possible overlap effect have caused some new tools to languish unused, while teams revert to fighting threats with the tools they already know.

One in five reports being only “somewhat confident” in their knowledge of the tools in their stack. And while 81% of surveyed respondents use less than 25 tools, 45% have already started to consolidate vendors and 21% may look into managed security services.

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



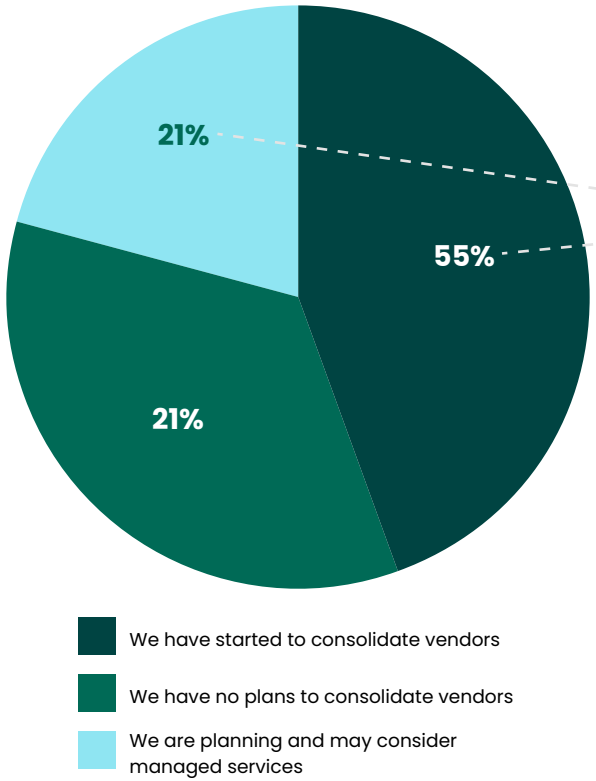
Tools & Vendors

CYBERSECURITY TOOLS AND VENDORS

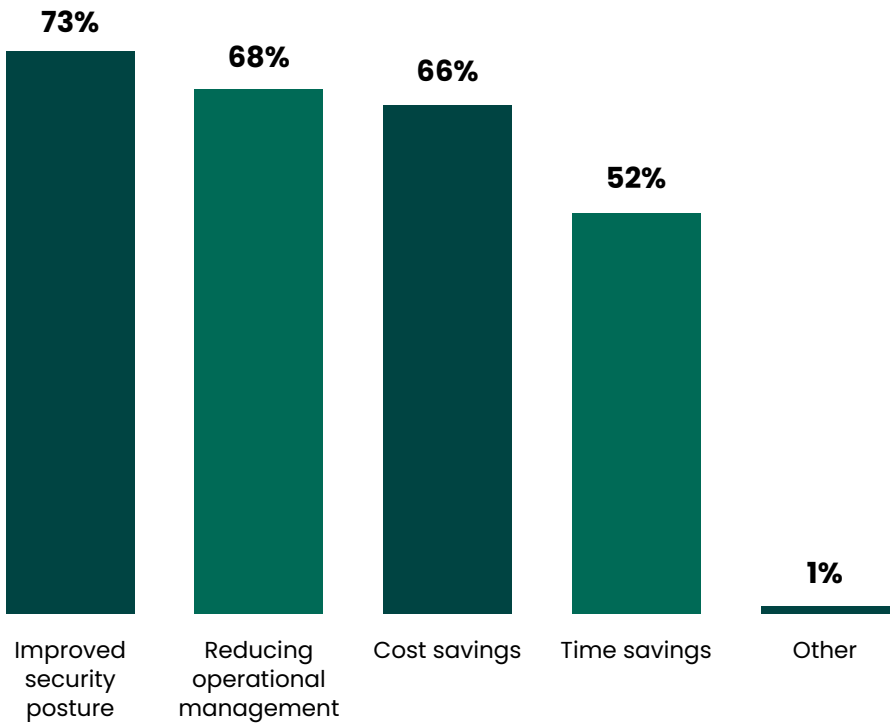
We're hitting a dichotomy here. Companies want best-of-breed products, but every bit of overhead adds up. New SLAs, new teams, meetings, onboarding routines, expectations, POAs, and even invoicing policies add to the confusion and overwhelm. Sticking with one vendor eliminates those problems, but then you fear your vendor is the "master of none".

At Fortra, we've taken this difficulty into account and have expanded, merged, and acquired to make ourselves the purveyor of best-in-breed security products all housed under one administrative umbrella and delivered by a single vendor. Check out our portfolio to see the difference ›

Where are you in your vendor consolidation journey?



What are your top drivers for vendor consolidation?



Staffing

STAFFING AND MANAGED SERVICES

Companies are coping with staffing shortages in different ways. As we mentioned earlier, one significant trend to come out of the cyber talent crisis is a generation of cybersecurity experts who have been forced to wear many hats — and be good at them. While there may not be someone with the luxury of only specializing in ransomware anymore, there are a lot more hands on deck that can contribute when they need to, and everyone is cross trained.

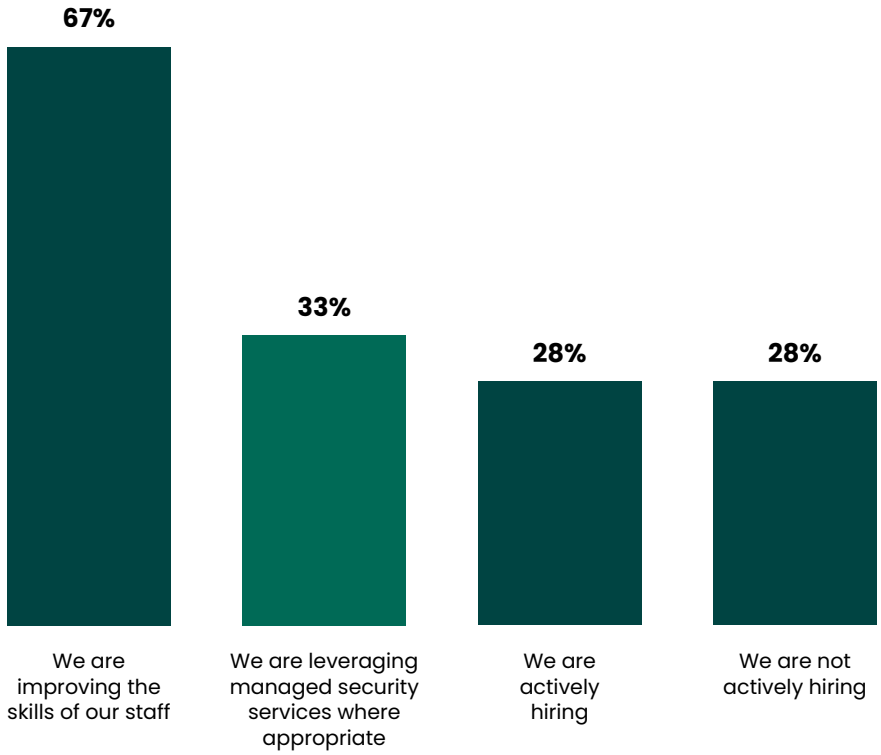
In line with these movements, the vast majority are focusing on improving the skills of their staff (67%).

Organizations are also leaning into managed security service providers (MSSPs) to offload some of the weight. While this may not free up enough time to make everyone a siloed expert again, it can take enough of the burden off of mundane tasks that key players can start to specialize again, at least where roles are concerned, and build up their in-house expertise. The most popular areas to offload? Email security and anti-phishing (58%), vulnerability management (52%), data protection (51%), and compliance (40%) took top spots.

An equal amount are hiring (28%) and not hiring (28%).

Avoid security configuration errors. Partner with cybersecurity experts who can identify issues before threats materialize. Discover Fortra managed security services ›

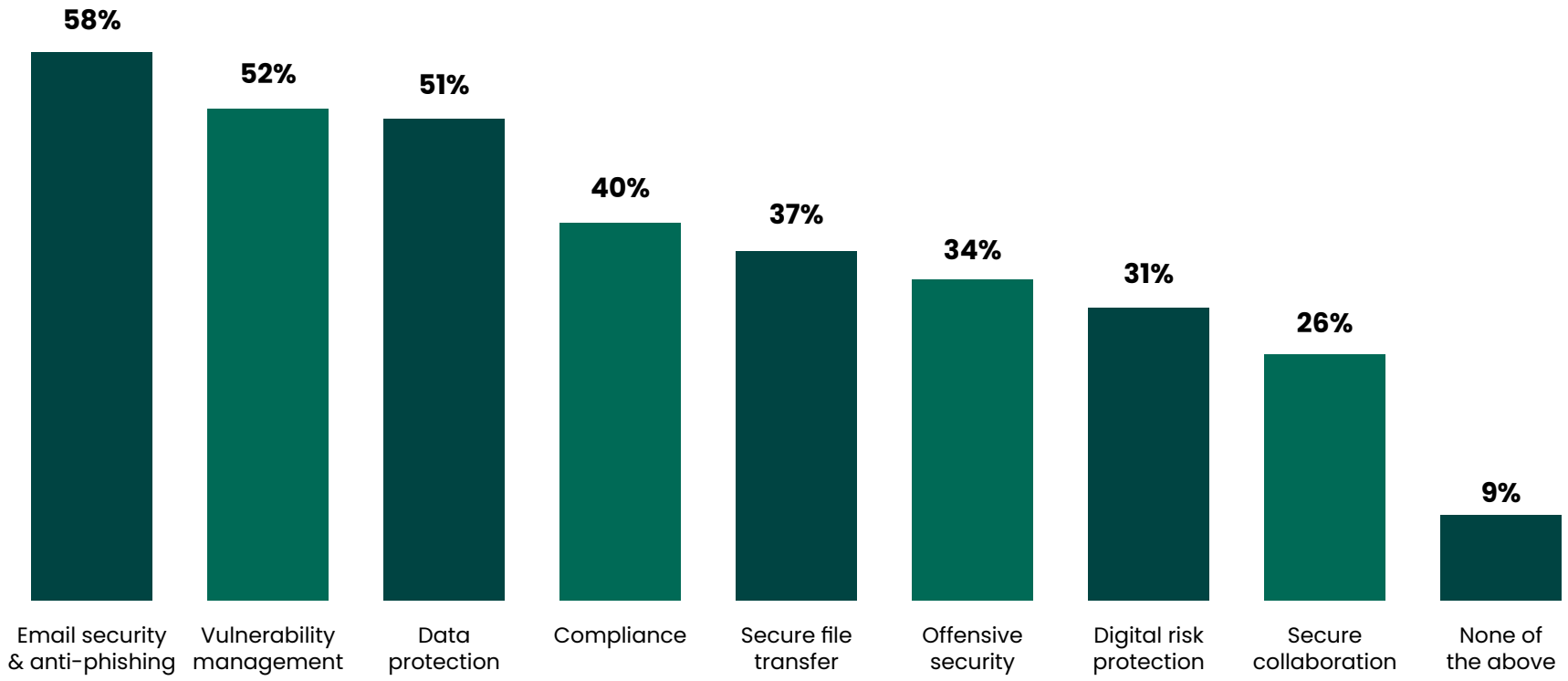
What best describes your cybersecurity staffing strategy? Select all that apply.



Staffing

STAFFING AND MANAGED SERVICES

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

Our survey respondents came primarily from eleven different industries, with "Other" (17%) accounting for over thirty more.

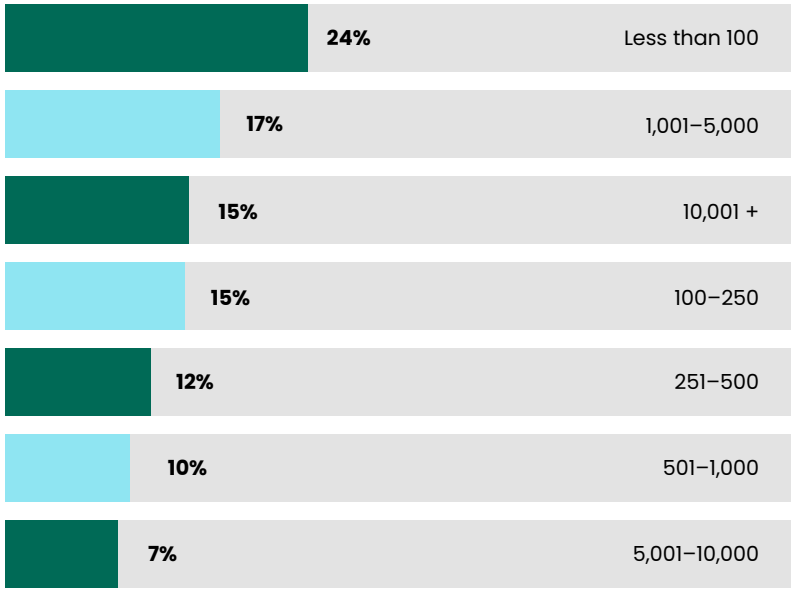
Those top industries included:

- Technology (25%)
- Banking and Finance (14%)
- Government (11%)
- Manufacturing (9%)
- Software Development (7%)

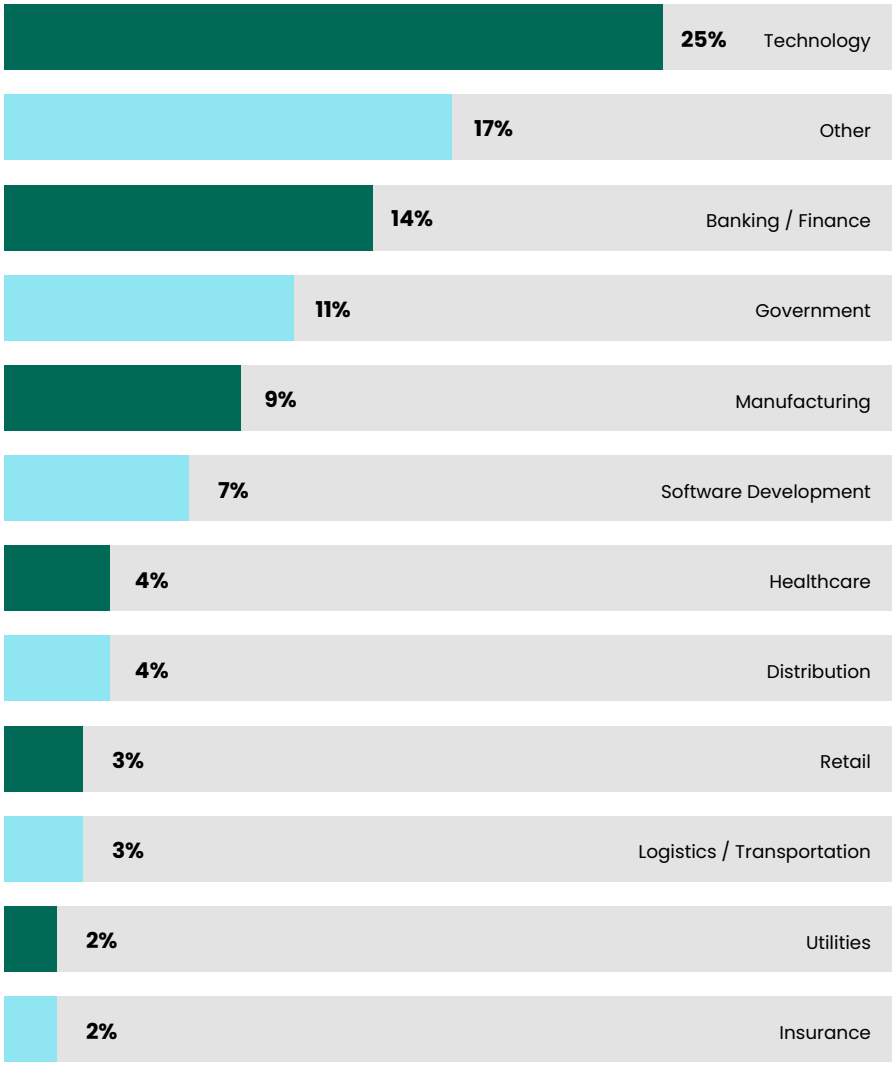
With "Other" industries extending from education to hospitality to real estate and beyond.

Nearly a quarter of organizations had less than 100 employees, 15% had up to 250, 12% had up to 500, and 15% were enterprises with over 10,000 employed.

How many employees does your organization have?



What is your organization's primary industry?



Demographics

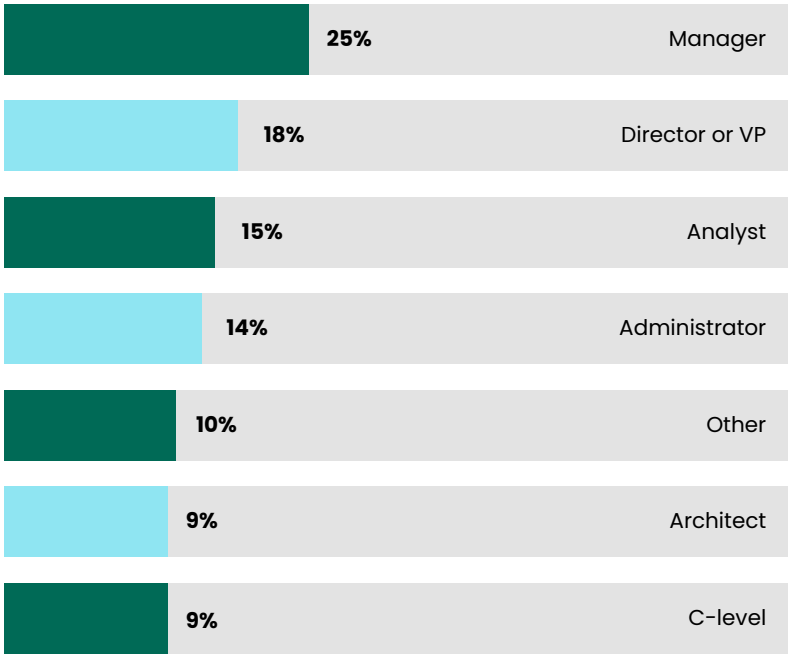
LOCATION AND JOB FUNCTION

Most of our survey respondents were from management (25%), with the subsequent breakdown as follows: Director or VP (18%), Analyst (15%), Administrator (14%), Other (10%), Architect (9%), and C-level (9%).

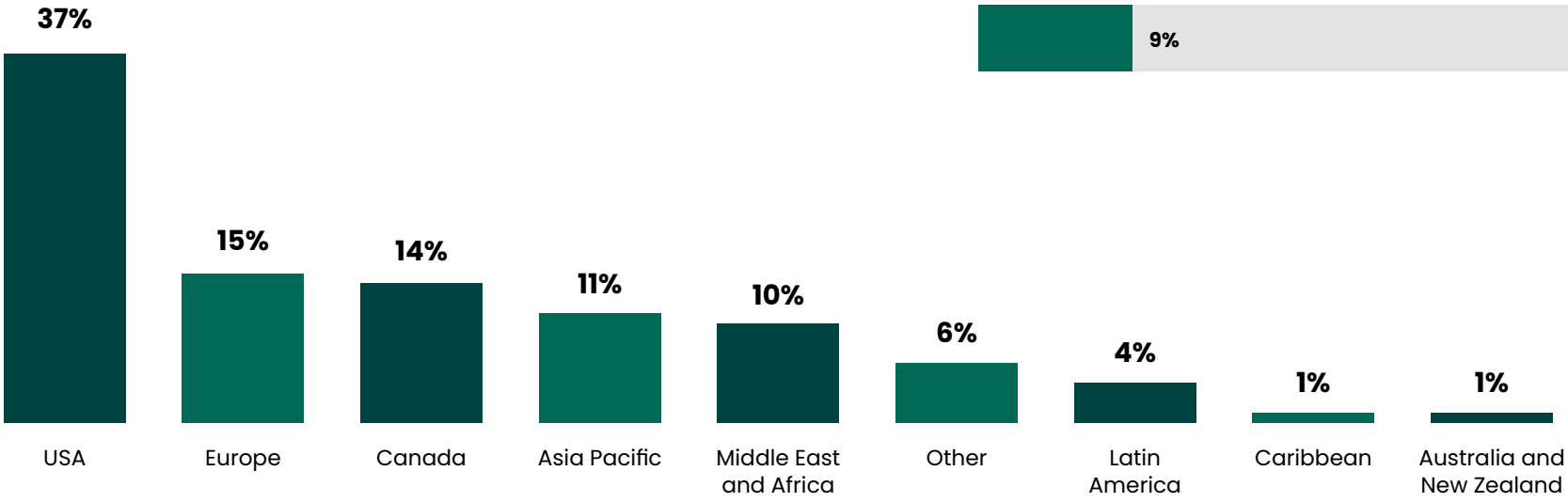
Participants came from the following regions:

- United States (37%)
- Europe (15%)
- Canada (14%)
- Asia Pacific (11%)
- Middle East / Africa (10%)
- Other (6%)
- Latin America (4%)
- Caribbean (1%)
- Australia / New Zealand (1%)

What is your job function?



Where are you located?



Closing Remarks

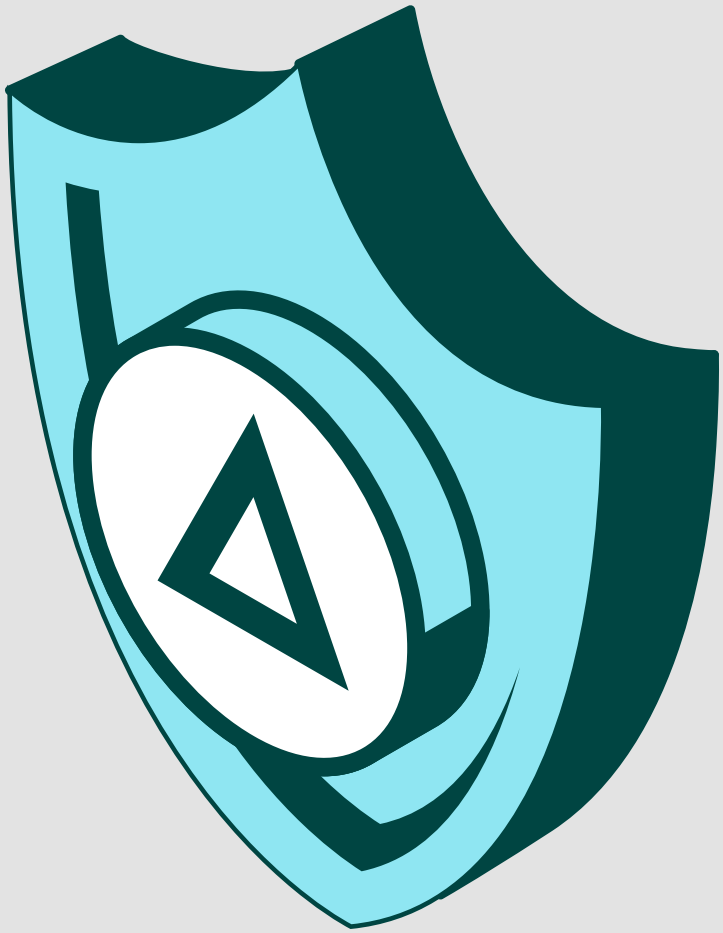
We are witnessing a crucial moment in which organizations are determining their digital trajectories for years to come. When facing these decisions, it's important to have a guide. Fortra knows the challenges today's companies face, and we make it our mission to provide the answers while still keeping it simple. We bring together specialized vendors and niche technologies, so when you consolidate with us, you get best-in-breed solutions all in one place. That's what sets us apart, and what makes a relationship with Fortra so special.

This 2024 Fortra State of Cybersecurity Survey is designed to level-set expectations for the security climate going forward and cut through the buzzwords, jargon, and noise. The candid responses from cybersecurity experts fighting in the trenches all over the world should be of note to any security decision-maker at the start of this new year.

While the specific takeaway will be different for each organization, we'd like to offer some final survey-driven recommendations that can apply to everyone. First, do the basics well. Though technology is rapidly advancing, cybercriminals will still try the door handles before breaking a window. Next, focus on your vital few. Never before has there been such a comprehensive digital overhaul in so short a timeframe: prioritize what matters most in your strategy, do it well, and then systematically move on. And lastly, invest in your people. Though the tools are improved, nothing can take the place of enough skilled analysts that can do the job. Today, "the job" includes learning the tools, growing the strategy, and scaling operations.

In one of the most exciting eras of cybersecurity development, Fortra is committed to staying on the front lines with you, every step of the way.

Our team is ready to answer your questions – we'd love to hear from you! Contact us today ›



FORTRA™

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-0124-db