RESEARCH REPORT

2022 State of Cybersecurity

September 2022

CompTIA

Introduction

Over the past year, the business world has been adjusting to lessons learned from the COVID pandemic. On a workforce level, companies are struggling to decide the best ways to balance employee flexibility and corporate culture. On a technical level, the many benefits of a cloud-first architecture are being weighed against the challenges of managing complexity and cost in a multi-cloud environment. It will still be years before we understand what equilibrium looks like in the post-pandemic environment, but the early changes point to a significant restructuring.

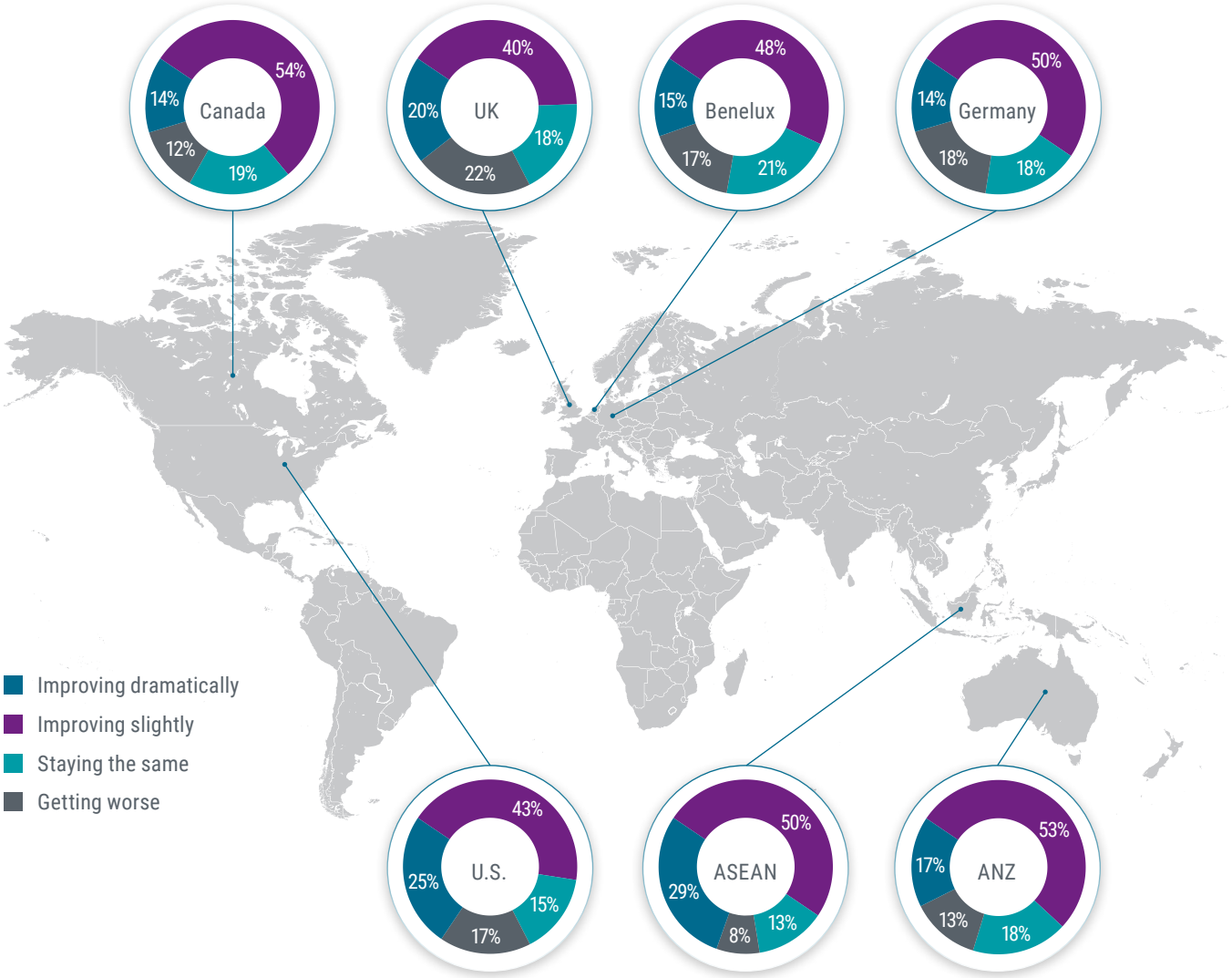
Another prominent takeaway from the pandemic is that symptoms are often easier to diagnose and treat than root causes. This obviously has implications beyond corporate strategies, but a prime example of this concept in the business world is the field of cybersecurity. Companies are made all too aware of poor cybersecurity when they are breached, and a postmortem can identify processes or tools that would have prevented or mitigated the attack. But that may not address underlying problems that can lead to a different cyber incident down the road.

CompTIA's 2022 State of Cybersecurity report examines the disconnect between root cause and symptoms. Digital transformation driven by cloud and mobile adoption is forcing a new strategic approach to cybersecurity, but fully adopting this new approach poses significant challenges, both tactically and financially. Although cybersecurity remains one of the most pressing issues for modern business, the hurdles that come from legacy views of IT and low understanding of the threat landscape make it difficult to follow the prescribed treatment.

Sentiments around cybersecurity are a good indicator of how difficult it is to make progress. Seven different geographic regions participated in CompTIA's 2022 State of Cybersecurity study, representing a range of economic and technical maturity. Across all seven regions, there is a clear belief that cybersecurity remains a problematic area, as both a general concern and a company-specific dilemma.

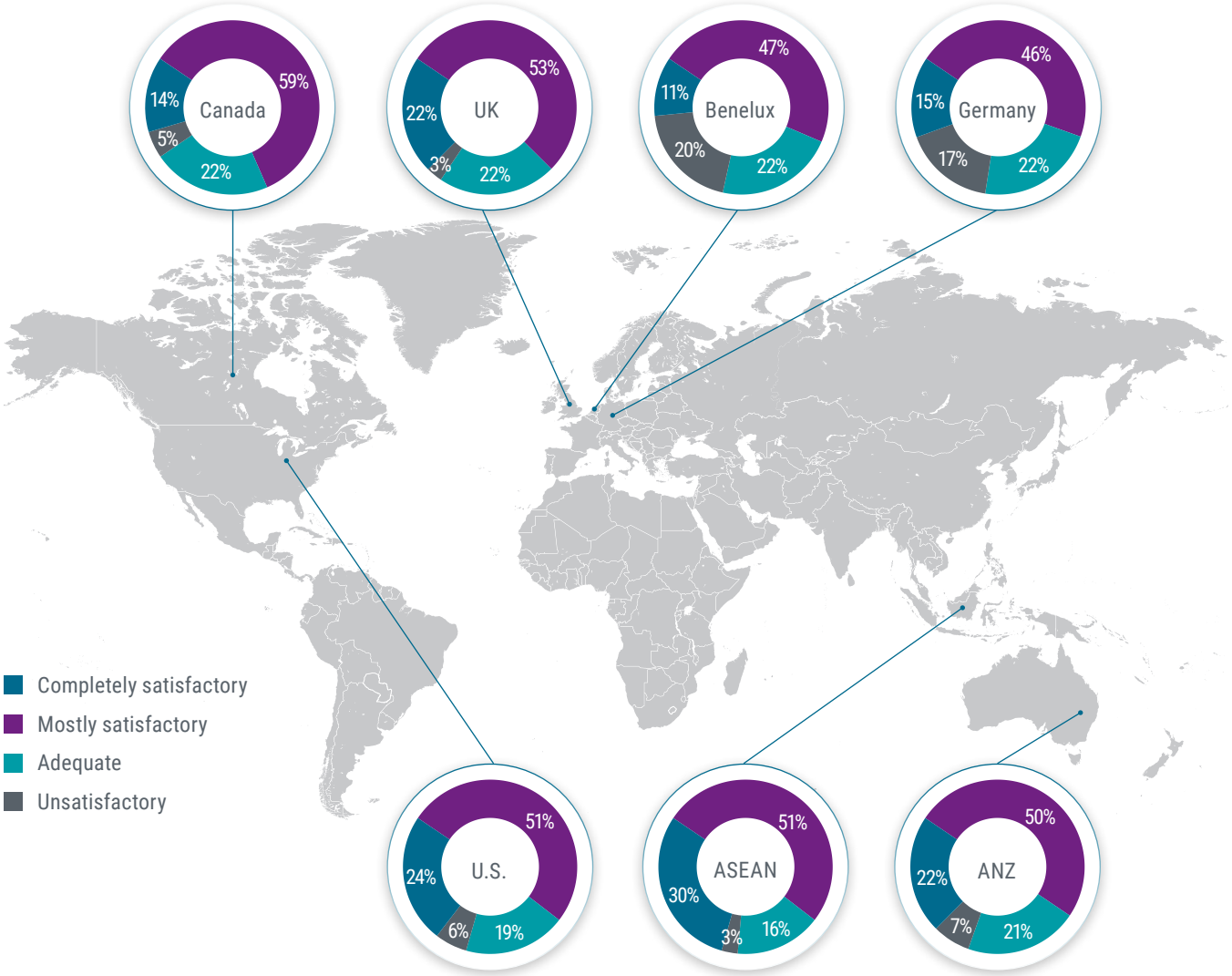
For starters, the general state of cybersecurity – which may include the organization of cybercriminals, governmental responses or the capabilities of available cyber defense mechanisms – is making relatively slow progress. Especially in more developed regions, few individuals believe that there is dramatic improvement being made. In most cases, nearly the same percentage of people believe that the situation is getting worse. While year-over-year data is not available outside the United States, the trend does not appear to be positive; the overall percentage of U.S. respondents who saw improvement in the cybersecurity landscape dropped slightly from 69% to 68%.

Global Cybersecurity Outlook



Bringing things closer to home, the view is not much better at the individual company level. While a majority of respondents in every region felt that their company's cybersecurity was satisfactory, a much smaller number ranked the situation as completely satisfactory. Nearly everyone feels that there is room for improvement, with some cases more dire than others. Here, the year-over-year trend shows some mixed signals. In the United States, net satisfaction rose (from 70% to 75%), but the rating of complete satisfaction dropped (from 29% to 24%). For the remainder of this report, the focus is on U.S. data. Separate research briefs highlight data points from international regions.

Organizational Cybersecurity Satisfaction



Throughout the pandemic, organizations accelerated the pace of technical adoption as they adjusted to historic disruption. This opened the doors for increased flexibility and long-term efficiencies. At the same time, that acceleration forced many companies into a space where traditional cybersecurity mindsets and tool kits were inadequate. Rather than addressing isolated concerns around specific activities, businesses have to adopt a new paradigm that informs cybersecurity decisions across the full range of operations.

Trends to Watch 2022

1 Policy

Cybersecurity becomes more integrated with business operations

2 Process

Zero trust tactics are used to move the needle

3 People

Organizations focus on specialization and enablement

4 Product

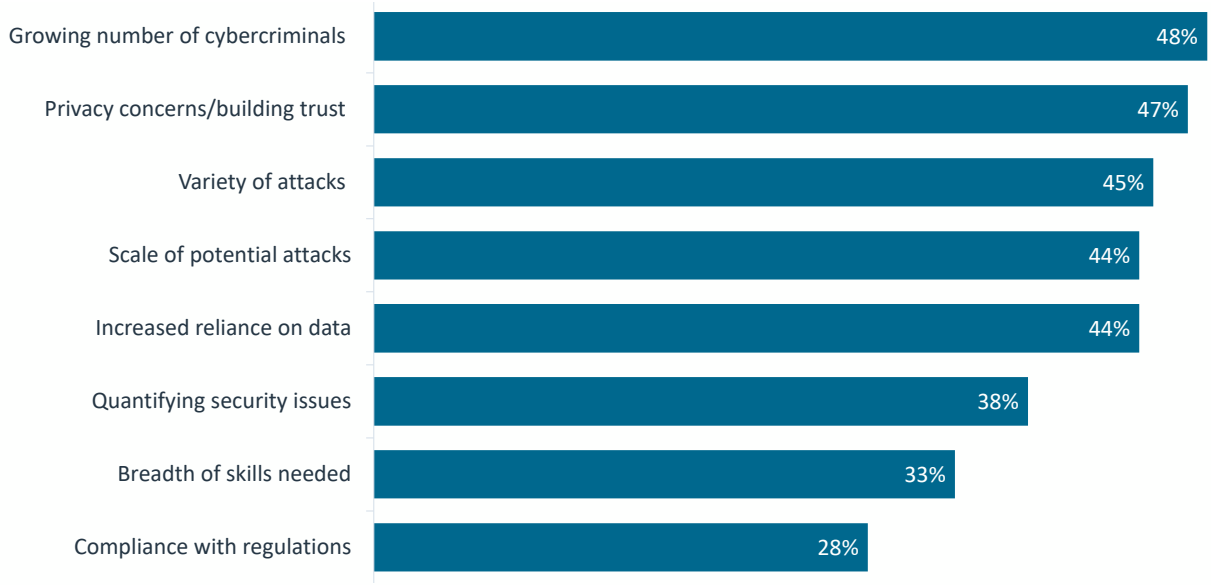
Automation reduces complexity but poses new challenges

Market Overview

In many ways, the field of cybersecurity is a reaction to the ways that enterprise IT evolves. After all, the need for cybersecurity only comes after technology has been implemented. This dynamic has intensified in recent years, as businesses aggressively pursue technology with the tendency to treat cybersecurity as a secondary consideration.

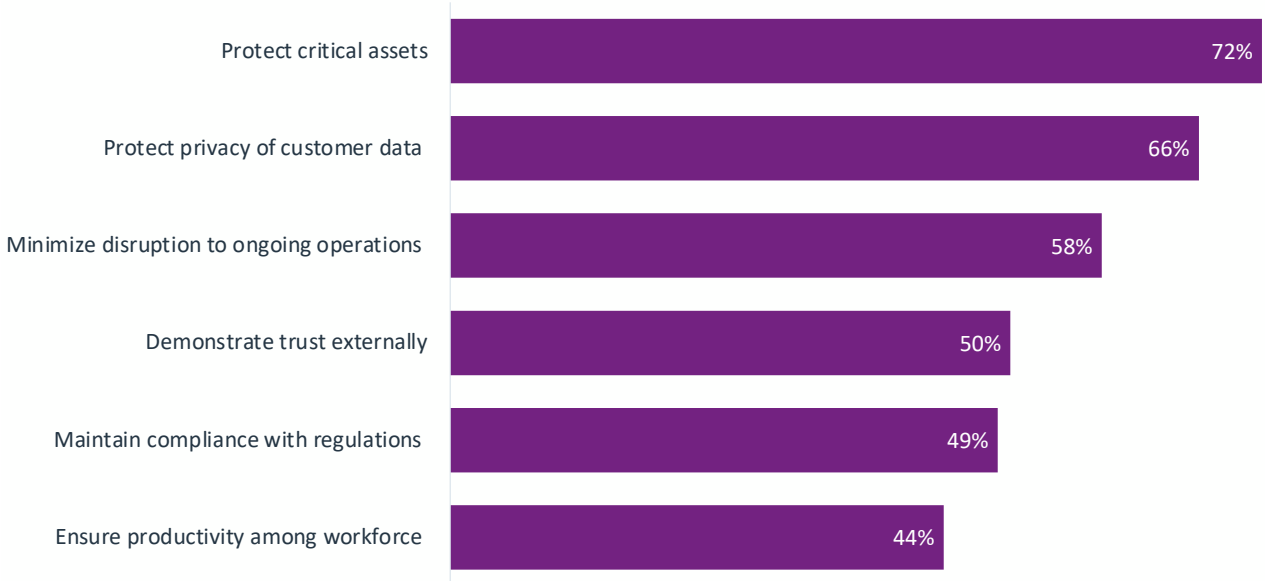
To the extent that the shape of cybersecurity follows the shape of IT, the defining characteristic of modern cybersecurity is complexity. Just as IT operations and strategy have grown more complex with the introduction of cloud and mobile systems, the management of cybersecurity has developed many facets as companies deal with the expansion of the threat landscape. According to CompTIA's survey, two of the top three issues driving cybersecurity are the growing volume of cybercriminals and the growing variety of cyberattacks.

Issues Driving Cybersecurity



Complexity demands clarity. With multiple factors impacting cybersecurity efforts – such as digital transformation, government regulation or customer perception – it is no longer sufficient to view cybersecurity as merely a protective coating. Organizations must carefully consider the objectives driving their cybersecurity strategy, which leads to probing questions. How does cybersecurity advance the interests of a business? How is cybersecurity success being measured? How are the proper investments being determined?

Objectives of Cybersecurity Strategy



Answering these questions, especially the last one, is leading to an ever-increasing focus on cybersecurity as a standalone discipline. If cybercrime is growing dramatically as a financial and operational liability, dedicated focus is the prescription for avoiding serious consequences.

Three data points describe the explosive nature of the cybersecurity landscape. First, Cybersecurity Ventures reports that the global financial damages from cybercrime totaled $6.1 trillion in 2021. This number is expected to grow 15% year-over-year, reaching $10.5 trillion by 2025. The costs of cybersecurity incidents go beyond the recovery of stolen data or the payments made due to ransomware attacks. Reputational damage can have large ripple effects, such as lost business from customers leaving or time spent negotiating new contracts if partners and suppliers lost faith.

To avoid becoming a cyber-related headline, businesses are increasing their cybersecurity budgets. Gartner projects that global cybersecurity spending will increase from $150 billion in 2021 to $172.5 billion in 2022, eventually growing to $267.3 billion in 2026. Much of this growth will be driven by spending on cloud security, as organizations continue migrating toward a cloud-first architectural approach. Secure identities will also be a major talking point, especially as companies consider blockchain-enabled identity solutions or identity-related implications for metaverse applications.

Finally, there is critical demand around cybersecurity skills. CyberSeek, a joint project between CompTIA, labor analysis firm Lightcast, and the National Initiative for Cybersecurity Education (NICE), shows that there are over 714,500 job postings in the United States requesting cybersecurity-related skills. Many of these openings are for dedicated cybersecurity positions such as cybersecurity analysts or penetration testers. CompTIA's State of the Tech Workforce report shows that demand in those areas will remain strong, with 4% growth expected in 2022 and growth that's expected to be 253% above the national rate over the next 10 years. According to Lightcast, the overall U.S. labor market is expected to grow 1% in 2022 and 7.8% over the next 10 years.

The scale and scope of the cybersecurity problem is immense, and no organization is immune to a disruptive attack. From government agencies guarding critical infrastructure to sole proprietorships protecting customer data, every institution in the digital era has to give cybersecurity its full attention. Past practices may be holding many companies back, but there are more resources than ever to help establish policies, build processes, train people and implement products in order to create the strongest possible cybersecurity posture.

One of the best resources organizations can use to stay on top of cybersecurity trends is an information sharing and analysis organization (ISAO). The CompTIA ISAO is an example of such an organization, focused specifically on cybersecurity trends that impact firms in the technology industry. In addition to threat intelligence and threat feeds sourced from top vendors and government agencies, the CompTIA ISAO provides networking opportunities for managed service providers and technology vendors to share best practices in implementing cybersecurity solutions and managing customer needs.

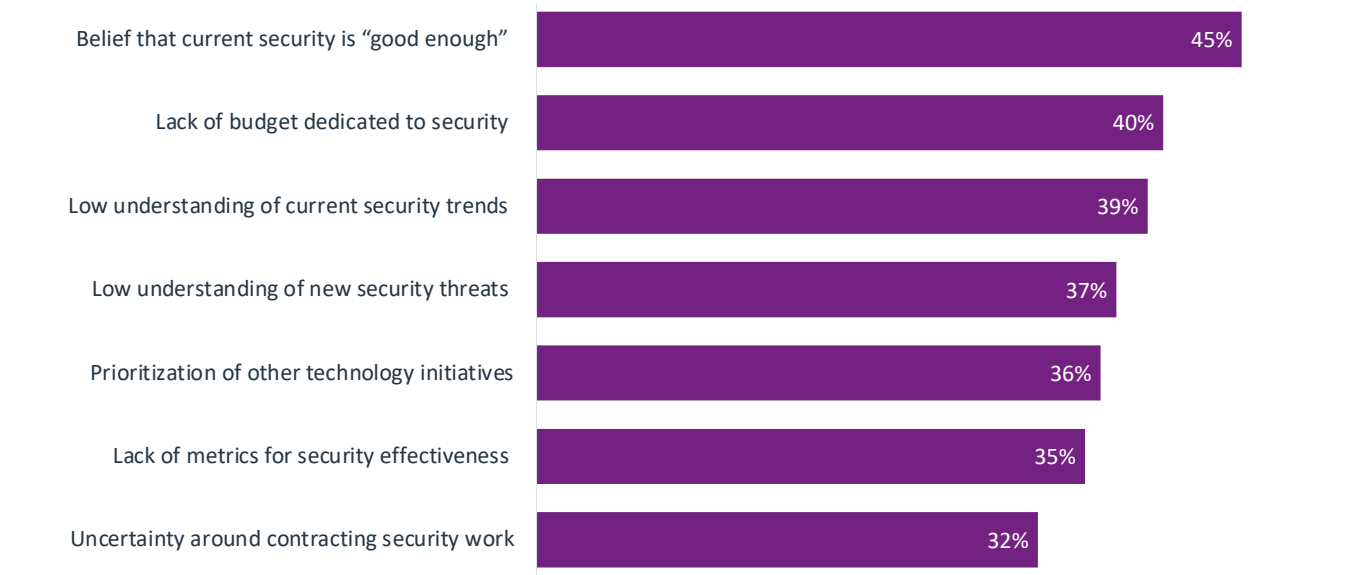
1 Policy

Another way that cybersecurity mirrors the evolution of enterprise IT is that both have become more strategic. When it comes to overall IT, organizations are generally embracing the transition to a more strategic approach, even if there are some growing pains along the way. Cybersecurity, on the other hand, is proving a bigger challenge when it comes to adopting a strategic mindset.

One of the most significant parts of a strategic mindset is recognizing that cybersecurity is no longer focused primarily on external events. Going back to the issues driving cybersecurity, most of the top issues cited are outward-facing. The focus on volume, variety or scale of attacks is a focus on things happening outside the business. Even concerns around privacy are concerns around external expectations. There is lower recognition that cybersecurity is attached to the changing nature of internal operations, such as a growing reliance on data or a need to maintain compliance with changing regulations.

Over the next year, there will be a concentrated move toward integrating cybersecurity with business operations. Accepting cybersecurity as a critical component of digital transformation will drive new questions and new measures of success throughout the organization. At the same time, adopting a holistic viewpoint will address many of the existing hurdles around changing the approach to cybersecurity.

Hurdles for Changing Approach to Cybersecurity

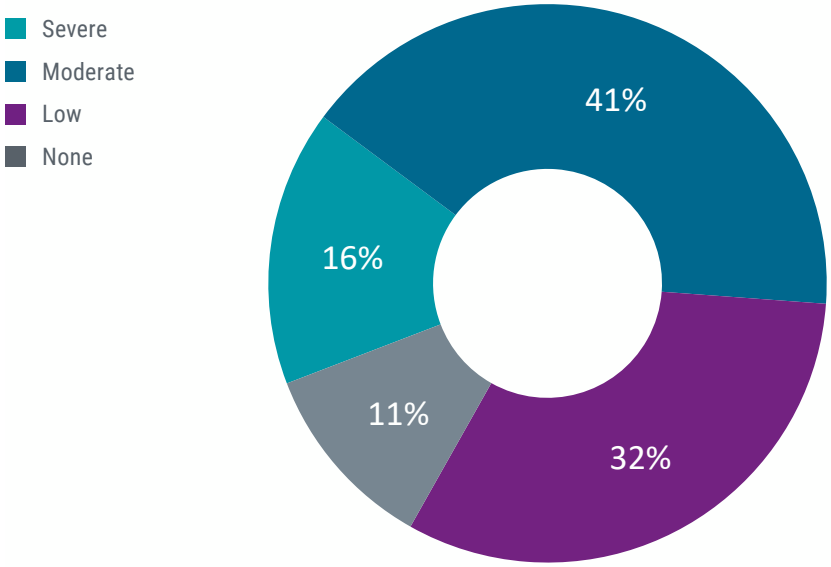


The primary hurdle companies have recently cited is a belief that the current cybersecurity posture is "good enough." This hurdle suggests two different assumptions that get challenged with a more strategic mindset. First, the notion of "good enough" indicates a lack of specific metrics around measuring cybersecurity efforts. For several years, CompTIA's surveys have shown a consistent need to establish more suitable and targeted cybersecurity metrics. Second, the simple qualification around cybersecurity being "good enough" is most commonly centered on whether or not a data breach has occurred. Beyond defining metrics, companies have to establish specific, strategic objectives around cybersecurity.

The second hurdle is a common thread through all areas of IT as technology becomes less tactical. Rather than holding budgets flat, organizations are finding that technology investments need to increase. Of course, this is another step that requires new metrics. Calculating return on investment is new ground for all areas of technology; it is an even bigger challenge for cybersecurity, where positive outcomes are less well-defined.

The next set of hurdles deal with cybersecurity expertise. Whether it is knowledge of general cybersecurity trends that may shape business decisions or specific cybersecurity threats that may require upgraded defenses, organizations need to improve their cybersecurity savvy. This will look different for different areas of a business, and the People section of this report takes a closer look at needs for various parts of the cybersecurity chain.

Impact of Cybersecurity Incidents



Although cybersecurity incidents alone are not a sufficient measure of a cybersecurity posture, they still provide a window into the need for strategic thinking. Among companies that recognized the occurrence of a cybersecurity incident in the past year, 57% said the incident had a severe or moderate impact on the organization, with 16% classifying the impact as severe. Aside from purchasing new software or hardware to address the incident, the largest component of mitigation efforts is the time spent by technical staff in resolving the issue.

Clearly there is an opportunity cost to time spent on incident response. Especially in an era of digital transformation, organizations are struggling to acquire and apply the skills needed for their technical objectives. Pulling resources away from innovative work in order to solve a preventable crisis is not a toll many businesses can afford. Taking a more proactive approach to cybersecurity efforts will minimize the impact of time spent on fire drills.

There is also a motivational cost in extra time spent on urgent cybersecurity issues. As security specialists are required to work overtime, it adds to mental strain that may already exist from a shift toward strategic IT, churn in the workforce or simply the global events of the past few years. In an environment where workers are prone to explore new opportunities, adding more stress is not in a company's best interest.

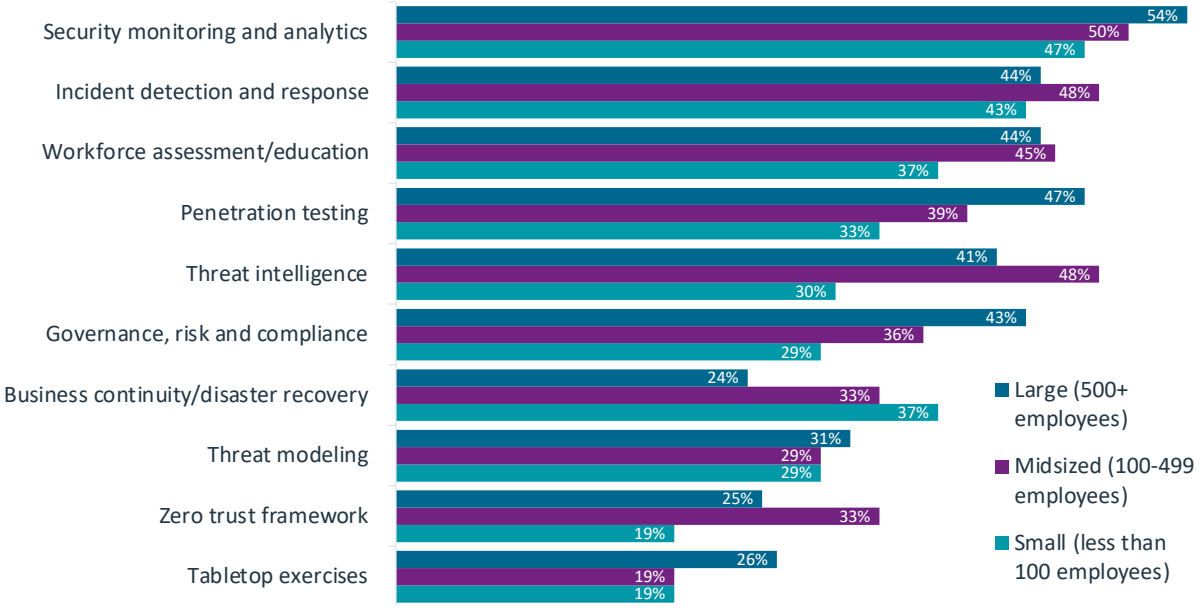
Ultimately, integrating cybersecurity more tightly with business operations will address many of the core problems companies face. With cybersecurity woven into the culture of an organization, there can be better processes with cybersecurity baked in, a more knowledgeable workforce with a lower tendency for inadvertent errors, and a comprehensive product set with support for a modern IT architecture. Time will tell if these changes lead to the elusive goal of higher satisfaction.

2 Process

Last year, CompTIA's State of Cybersecurity report identified zero trust as the overarching policy that should be guiding modern cybersecurity efforts. The introduction of cloud computing and mobile devices drastically altered the viewpoint of a secure perimeter, which had been the dominant mindset for decades. As organizations grappled with the paradigm shift, part of the difficulty was in defining a comprehensive approach that informed a wide range of cybersecurity decisions. Zero trust emerged as the answer to that dilemma.

This year, zero trust is starting to move from broad policy into tactical processes. For several reasons, adoption of zero trust will not take place overnight. First and foremost, zero trust represents a drastically different way of thinking about cybersecurity. Rather than viewing cybersecurity as one of many components within the IT function and simply investing in hardware or software, companies must now view cybersecurity as an organizational imperative, extending beyond technology products into decisions around workflow and workforce.

Cybersecurity Practices in Place

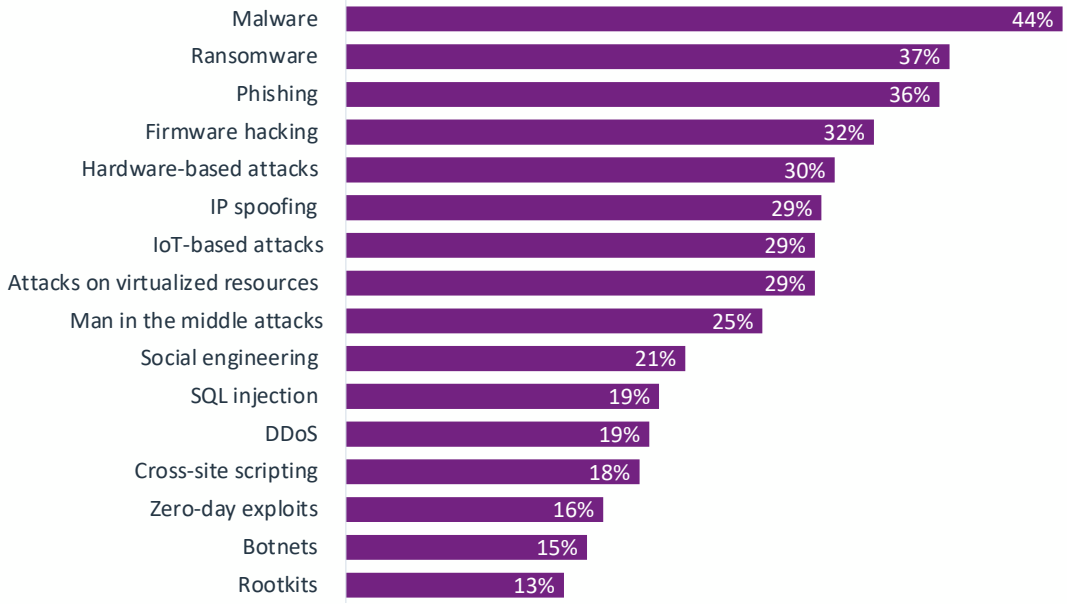


Building organizational awareness around zero trust will be a demanding task. Zero trust still ranks quite low as a cybersecurity practice within organizations, but this is partly because different areas of the workforce have different levels of familiarity with cybersecurity strategy. For example, a relatively low percentage of respondents – including only 24% of respondents from large companies – indicate that their organization has a practice around business continuity and disaster recovery (BCDR). The incidence of BCDR plans is likely much higher, but individuals within business units may not be required to understand any part of these plans.

In addition, zero trust is not a single product or action, and many discrete tools and practices can be part of a zero trust approach. Looking at components that typically fall under a zero trust umbrella, there are more organizations that recognize individual parts vs. the collective whole. Multifactor authentication, one of the best tools to validate trusted identity, is in place at 46% of organizations. Cloud workload governance, a process that ensures cloud resources are being used according to plan, is in place at 41% of organizations. Other elements, such as software-defined microsegmentation (38%) and least-privilege access (26%) have lower adoption, but adoption in those areas is still slightly ahead of broad awareness for a zero trust policy.

The main takeaway is that zero trust is a philosophy around cybersecurity that informs questions and decisions. The best way to adopt zero trust is not to define a set of criteria that indicate complete success, but to build a road map identifying the best steps to take based on the status of the organization. Those steps might include a full audit of data and workflow, implementation of specific products such as identity and access management (IAM) software, or creation of an ongoing workforce education program. Each step should address a specific question, and each step should have measurable outcomes.

Areas for Improvement in Threat Intelligence

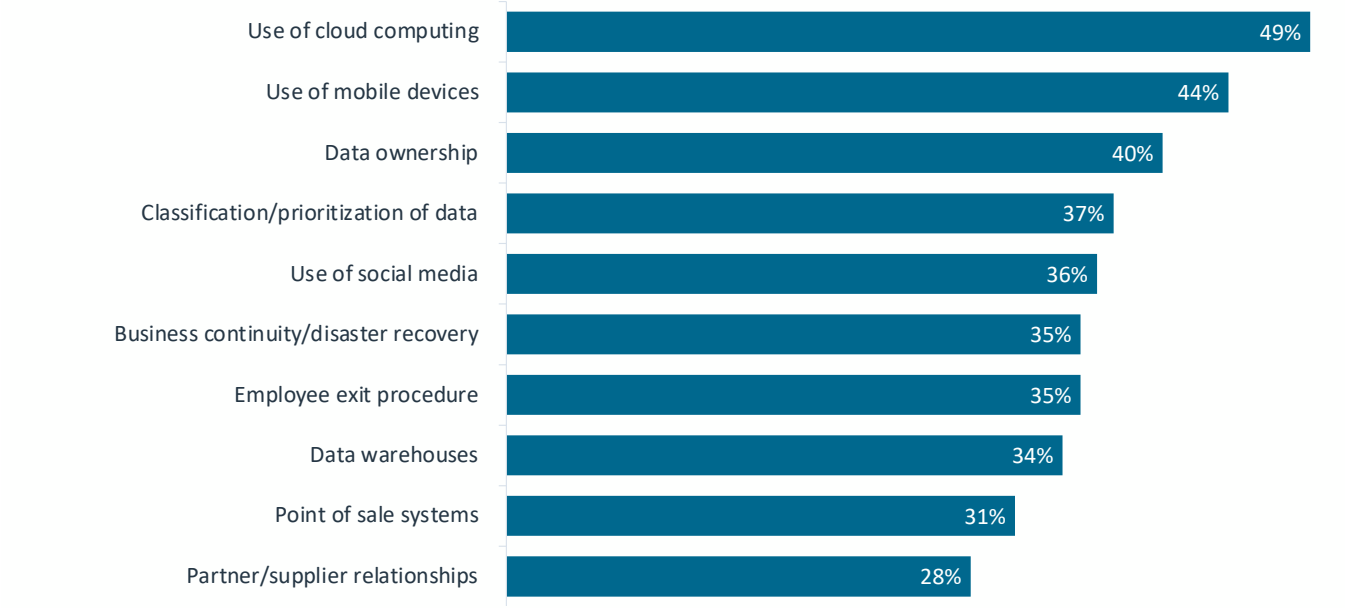


Within the many cybersecurity practices that will be affected by a zero trust approach, there are two areas that deserve special attention. Threat intelligence is the natural progression of cybersecurity's most traditional function. If a business wants to keep all the attacks from getting in, it needs to understand the nature of those attacks.

Threat intelligence is an exercise in balancing contrasts. Cybersecurity teams need a broad understanding of the threat landscape along with deep knowledge of how the most troublesome attacks are executed. Monitoring for cyber threats is an ongoing practice that requires rigor and scheduling, but there must also be the ability to act quickly in response to severe issues such as zero-day vulnerabilities or supply chain attacks. In many ways, threat intelligence has a foot in the old world of cybersecurity, with an emphasis on consistency and defense, and the new world, where flexibility and proactive response is critical.

The list of threats that companies want to better understand demonstrates the scope of the problem. Malware is the threat with the longest history, but it still ranks first since constant evolution requires constant attention. Ransomware and phishing have quickly become major areas of concern as digital operations have increased and human error has proven more costly. There are nine different threats causing concern to at least one quarter of all companies. Any one of the threats lower on the list could quickly become more pressing if it proves especially profitable to hackers. Improving threat intelligence in the future will require dedicated effort and broader participation in peer networks and ISAOs.

Components of Risk Management



The second area worthy of a closer look is risk management. Governance, risk and compliance (GRC) is identified as a current practice by only 35% of companies. The regulatory part of GRC may cause some firms to be dismissive of the practice (even though regulations around digital operations are rapidly changing), but the risk part should not be treated lightly.

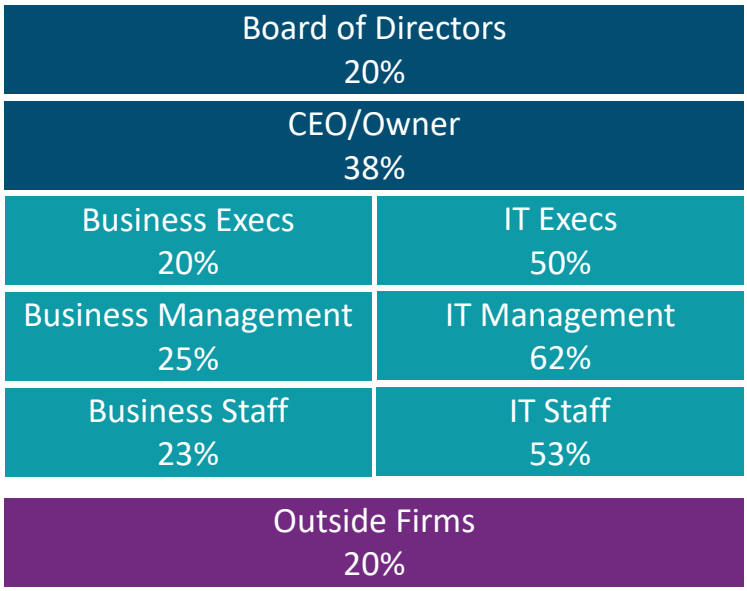
Formal risk analysis involves diving into the details of both technical and business operations. The days of the secure perimeter created a lackadaisical approach to cyber risk; information with any level of importance was simply put behind a firewall. Today there is no limit to the amount of security a company could impose on critical data, but there are certainly limits to budget and usability, making it impractical to give all data the highest level of security. Risk management, especially in the era of zero trust, starts with a thorough understanding of both corporate assets and business operations.

From there, risk management becomes a series of tradeoffs. What are the costs in securing cloud systems vs. the benefits of a resilient cloud architecture? How can mobile devices enable a flexible workforce without exposing corporate data? Which pieces of customer data are most critical for market analysis, and which pieces should not be collected? These questions are not purely technical. They require input from both business units and IT teams, and the process will be iterative as there are changes in business objectives and advances in emerging technology.

3 People

As businesses try to address the root cause of their security shortcomings, they discover that the problem has multiple layers. There is obviously the technical layer, which has been the focal point for years and continues to be a substantial part of a cybersecurity solution. There is also the workforce layer, and many companies have turned to cybersecurity awareness education to improve this aspect. However, other layers dealing with business operations and corporate measurements have likely received less attention in recent years.

Groups Involved in Cybersecurity Chain

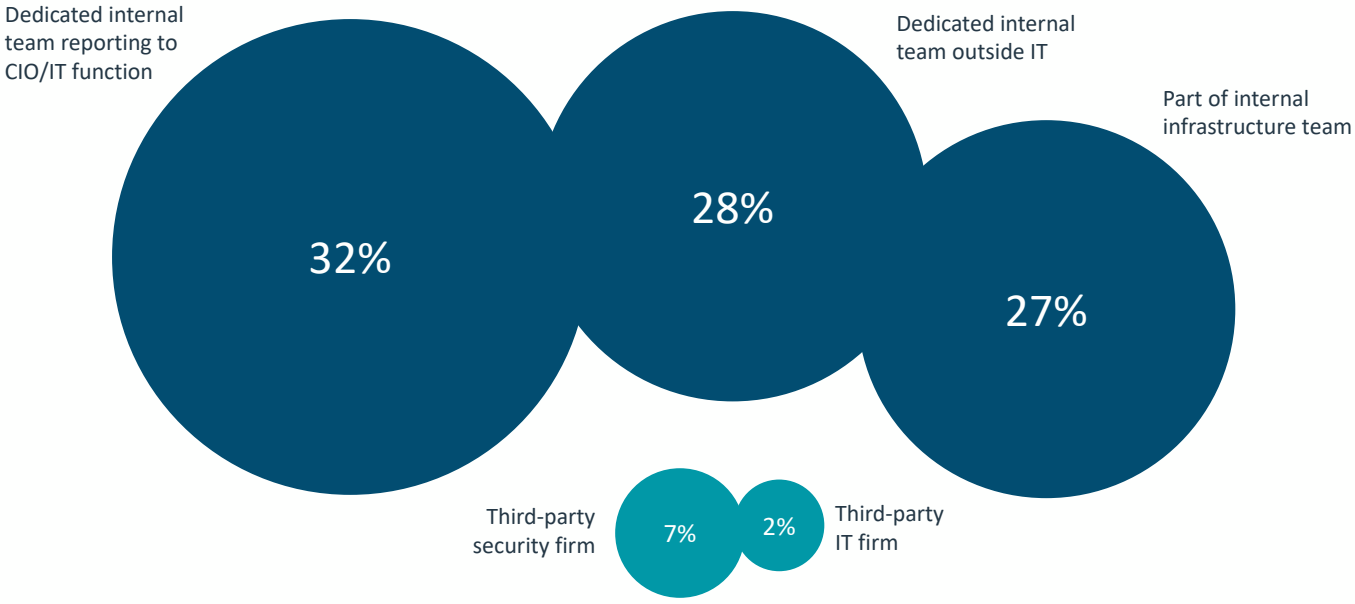


The participation rates within cybersecurity chains show which layers are getting less attention. A cybersecurity chain is all the stakeholders that take part in cybersecurity discussions, with the goal of tying these discussions together into a comprehensive strategy. As expected, most firms have high participation from the IT function. These numbers are dragged down slightly by smaller companies that may not have dedicated IT staff, but most companies would clearly have technical staff as part of the cybersecurity solution. At the same time, organizations that do not recognize IT staff as part of the cybersecurity chain may not even recognize that discussions should be taking place more broadly throughout the organization.

Where discussions are recognized, though, there is still low participation on the business side. Small businesses tend to have more engaged owners – 47% of small businesses have the CEO or owner as part of the cybersecurity chain compared to 37% of mid-sized firms and 27% of large enterprises – but the overall rate of business staff participation is too low for a business-critical function.

Not only are participation rates low across the board, but they are also not changing. From the board of directors to business staff to IT specialists to outside firms, all participation rates in this year's study are nearly identical to the rates in last year's study. Organizations are struggling to develop cybersecurity conversations that tie together tactical efforts with strategic vision.

Location of Security Operations Center

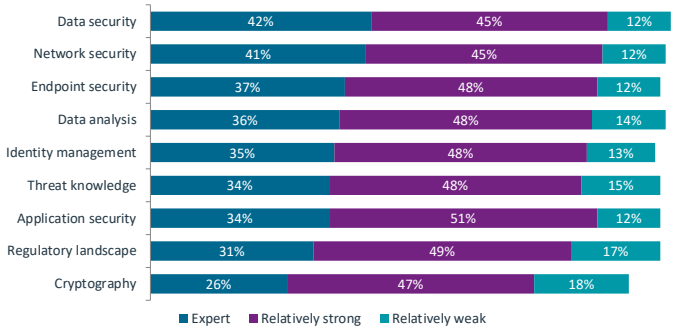


Cultivating the cybersecurity chain should be one of the primary functions of the Security Operations Center (SOC). The SOC is typically thought of as the group executing on cybersecurity tactics. For the vast majority of organizations, the SOC is an internal function. There is a clear trend toward establishing dedicated resources as part of a SOC, and there are early indications that more companies are moving the SOC outside the IT function. Regardless of location, SOC leadership should give more consideration to integrating cybersecurity into operational discussions at every layer.

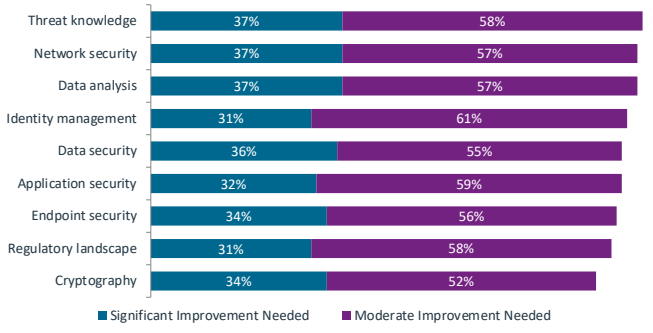
Of course, some companies may need to formally define their SOC in order to identity the leaders responsible for this task. While large organizations often have a chief information security officer (CISO) leading cybersecurity efforts, smaller firms may view their SOC comprising a single cybersecurity engineer or a few IT generalists with cybersecurity responsibilities. Constructing a SOC with a specific charter and assigning roles and responsibilities within the SOC will drive conversations forward and identify other strategic gaps that need to be addressed.

Regardless of how a company defines their SOC, technical specialists will always be a critical component. The supply/demand equation for cybersecurity skills has been out of balance for some time, and the situation shows little sign of improving in the near future. In addition to describing more than 714,500 job postings requesting cybersecurity-related skills, the CyberSeek project highlights the 12 months between May 2021 and April 2022, when there were 180,000 openings for information security analysts but only 141,000 workers currently employed in that role. Companies are fighting over a pool of talent that is not growing fast enough.

Assessment of Cybersecurity Skills



Cybersecurity Skill Needs



To improve institutional skills and knowledge, companies must first understand the current state of their cybersecurity workforce. Data from CompTIA's survey is only a rough estimate of current skill – business staff and even higher-level IT management may be disconnected from day-to-day work – but even a rough estimate is a good starting point for the discussion. Companies should take the next step and develop methods for performing more detailed assessments as they consider which skills to improve.

The list of skill needs from CompTIA's survey is further proof that the skill assessment is a rough estimate; some areas high on the list for improvement are also viewed as areas of high expertise on the assessment. The skill needs, though, may present a more accurate picture. Network security may seem like an area with deep expertise since the task has been performed for a long time, but the reality is that changes in the IT landscape demand constant improvement. Other areas such as threat knowledge, data analysis and identity management are more obvious candidates for skill growth since they represent more recent trends in cybersecurity.

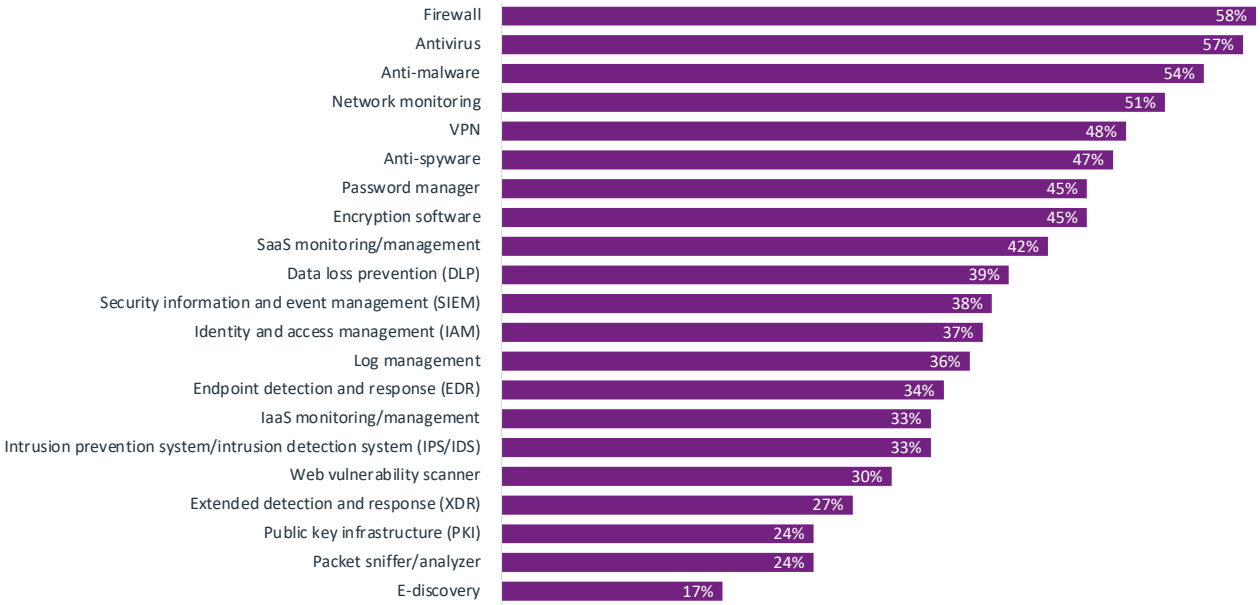
Companies can clearly not rely exclusively on hiring to fill their gaps. Finding the right fit on the open market is both challenging and expensive. Training is an option that should be utilized more heavily. Training for existing workers can target specific skills, deliver results more quickly and build loyalty among employees. As cybersecurity grows more complex, expanded partnering is also worth exploring.

Unfortunately, attracting or building the right skills is only half the battle. Retaining skills, especially in a high-demand environment, is a major undertaking. ISACA's State of Cybersecurity 2022 report found that 60% of companies were having difficulty retaining their cybersecurity professionals in 2021, a seven point jump from 2020. The good news is that many retention activities line up neatly with developing a strategic view of cybersecurity. The top challenge in managing cybersecurity resources, cited by half the respondents in CompTIA's survey, is providing the tools and support that allow staff to be effective. This may result in financial investment (as does the second challenge, paying market wages), but it can also be achieved with structural changes or new processes. The third challenge requires no financial investment at all but circles back to the main policy goal. Integrating cybersecurity with business initiatives is a root cause action that can address the symptom of cybersecurity professionals who feel disconnected from the organization.

4 Product

The toolbox of cybersecurity products is certainly not getting any smaller. While policy and process are the biggest levers companies can use to improve cybersecurity posture, software and hardware are still a necessary part of the solution.

Cybersecurity Products in Use



The cybersecurity product list starts with pieces that have been around for a long time. Firewalls, antivirus and anti-malware were the primary components of the secure perimeter, and they still serve that function even as the secure perimeter has dropped in importance. These tools are ubiquitous, although many end users (and possibly even IT staff) may not think of them as part of the product set since they are so common.

Network monitoring is another tool with a long history and one that is evolving to fit the times. Tools such as SolarWinds Network Performance Monitor, Datadog Network Monitoring and Auvik offer extensive capabilities for observing and analyzing an entire network architecture. Recent features in network monitors include visibility into cloud components of the network and analytical tools to better understand data flow.

Sticking with the cloud theme, SaaS monitoring and management tools saw a substantial jump in adoption, from 32% penetration in 2021 to 42% penetration in 2022. Acceleration in cloud adoption was one of the largest shifts in IT operations during the pandemic, and companies are now responding to the second-order effects of that activity. Along with cybersecurity issues, cloud systems come with a unique set of concerns around utilization and cost, and new management software is needed to properly administer, orchestrate and secure cloud architecture.

On the other end of the spectrum, there are tools that still have low adoption rates but should be strongly considered as imminent additions. Although SaaS is the most popular form of cloud adoption, IaaS is also prevalent and may be more critical for proper monitoring and management. Comprehensive network monitoring tools are crucial for providing a view of the big picture, but packet sniffers and LAN analyzers are targeted products that can root out hard-to-find problems.

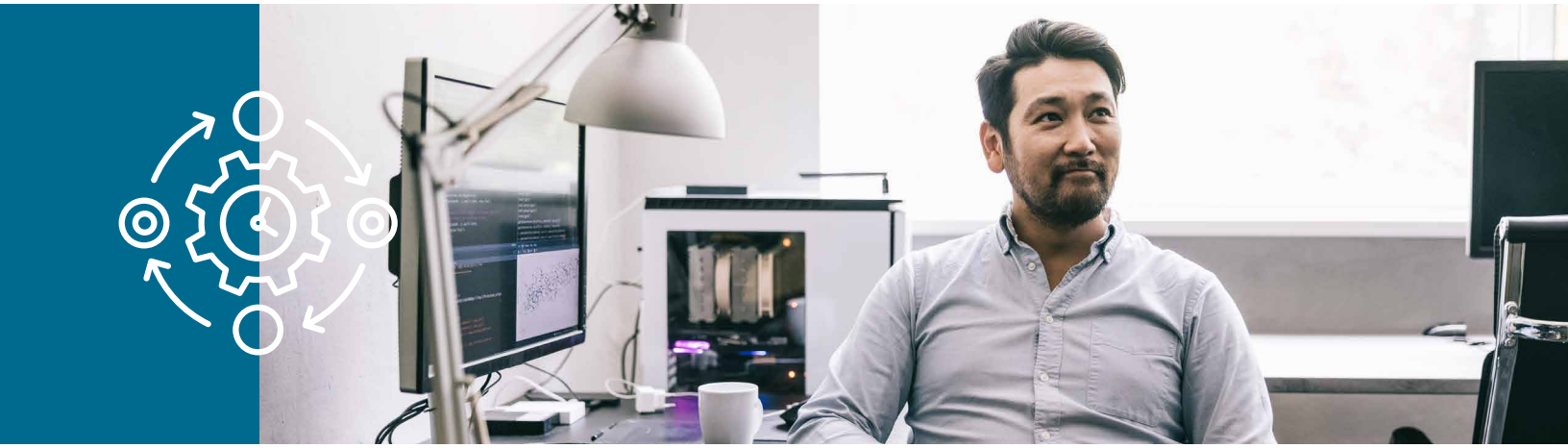
With so many tools in the arsenal and so many constraints on cybersecurity personnel, the obvious next step is automation. Previous research from CompTIA on the topic of automation sheds some light on how automation figures into a cybersecurity strategy. The research, conducted in Q2 2021 among 397 business professionals, shows that detecting potential cybersecurity incidents is the top example of automation initiatives being undertaken by companies today.
As with every other example of automation, there are two sides to the coin. On one hand, automation cuts through the high degree of complexity that is present in modern cybersecurity efforts. For this reason, many companies take an early view of automation as something that can directly address their personnel constraints. Just as companies hoped that automation and self-service could reduce the demand for tier one help desk support, they hope that automation can reduce demand for tier one work in the SOC.

However, the other side of the automation coin has to be considered. Automation itself is a complex endeavor. The top two challenges cited in the automation research are connecting IT systems and closing skill gaps. The scale and scope of modern IT architecture demands automation, but the available resources still have their hands full in implementing automation and monitoring the system to ensure that automation is working properly.

The assumption that tier one demands decrease is also faulty. Digital transformation has greatly increased the amount of technology used throughout an organization, the utilization of data for day-to-day operations, and the problems that can impede performance or create vulnerabilities. Automation does not remove tier one requests as much as it changes the nature of those requests. While simple issues like a password reset or a software patch may be handled through automation, the individual that previously handled those requests manually is now tasked with solving bigger problems.

Even if automation does not completely solve the resource issue, it makes the situation more manageable. Integrating cybersecurity with business operations makes cybersecurity even more critical than ever, and implementing a zero trust philosophy leads to a range of new processes. A dedicated organizational structure and the proper tool set are the first steps in tackling added complexity. By adopting a balanced approach to automation, organizations can fully address their underlying difficulties and move towards a healthy cybersecurity outlook.

Methodology



This quantitative study consisted of an online survey fielded to business and IT professionals involved in cybersecurity during Q3 2022. A total of 500 professionals based in the United States participated in the survey, yielding an overall margin of sampling error at 95% confidence of +/- 4.5 percentage points. For international regions (ANZ, ASEAN, Benelux, Canada, Germany and UK), a total of 125 professionals in each region participated in the survey, yielding an overall margin of sampling error at 95% confidence of +/- 8.9%. Sampling error is larger for subgroups of the data.

As with any survey, sampling error is only one source of possible error. While non-sampling error cannot be accurately calculated, precautionary steps were taken in all phases of the survey design, collection and processing of the data to minimize its influence.

CompTIA is responsible for all content and analysis. Any questions regarding the study should be directed to CompTIA Research and Market Intelligence staff at research@comptia.org.

CompTIA is a member of the market research industry's Insights Association and adheres to its internationally respected Code of Standards and Ethics.

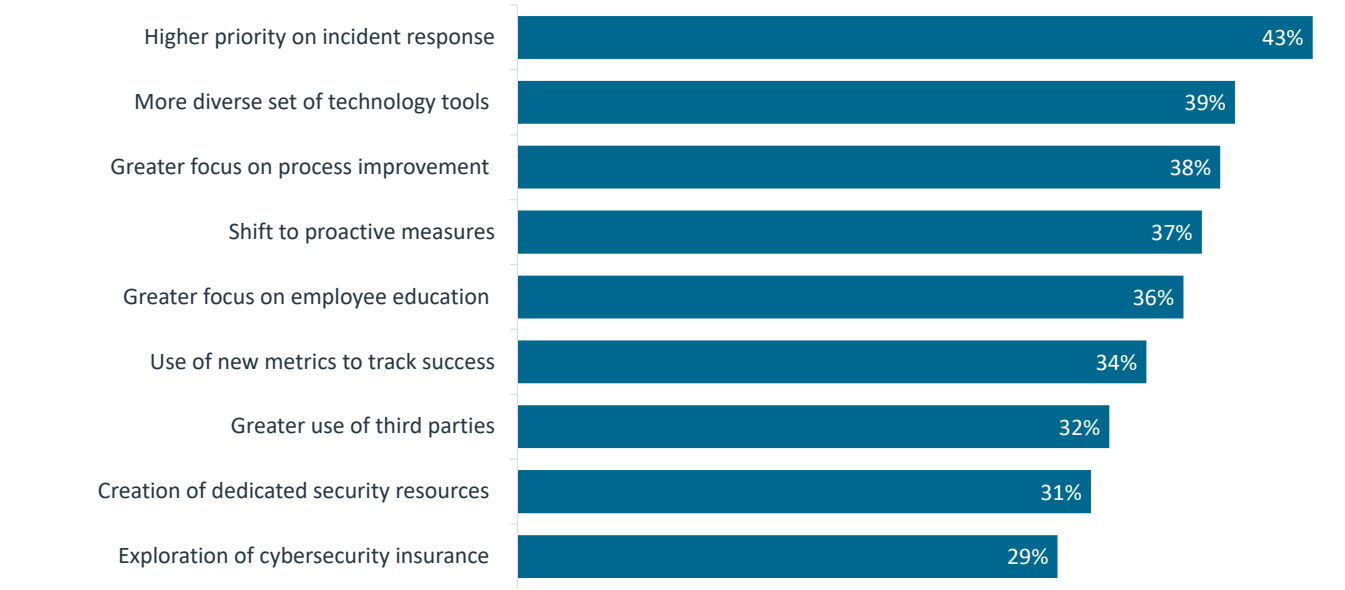
About CompTIA

The Computing Technology Industry Association (CompTIA) is a leading voice and advocate for the $5 trillion global information technology ecosystem and the estimated 75 million industry and tech professionals who design, implement, manage and safeguard the technology that powers the world's economy. Through education, training, certifications, advocacy, philanthropy and market research, CompTIA is the hub for advancing the tech industry and its workforce.

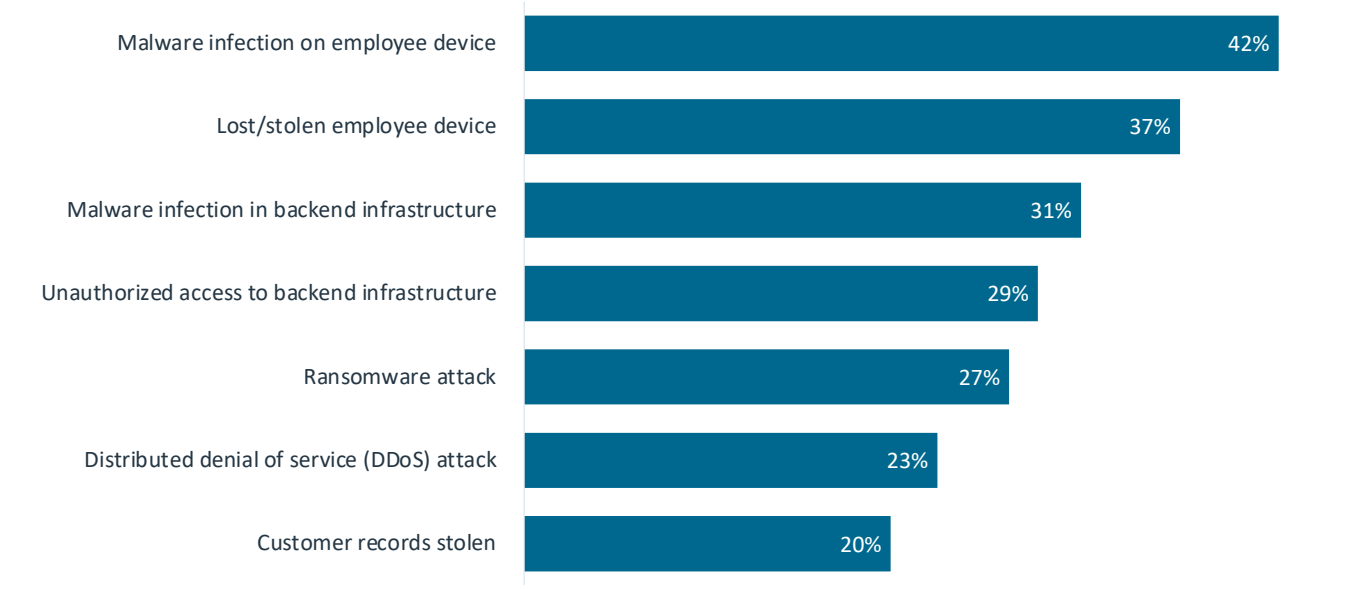
CompTIA is the world's leading vendor-neutral IT certifying body with more than 3 million certifications awarded based on the passage of rigorous, performance-based exams. CompTIA sets the standard for preparing entry-level candidates through expert-level professionals to succeed at all stages of their career in technology. Through CompTIA's philanthropic arm, CompTIA develops innovative on-ramps and career pathways to expand opportunities to populations that traditionally have been under-represented in the information technology workforce.

Appendix

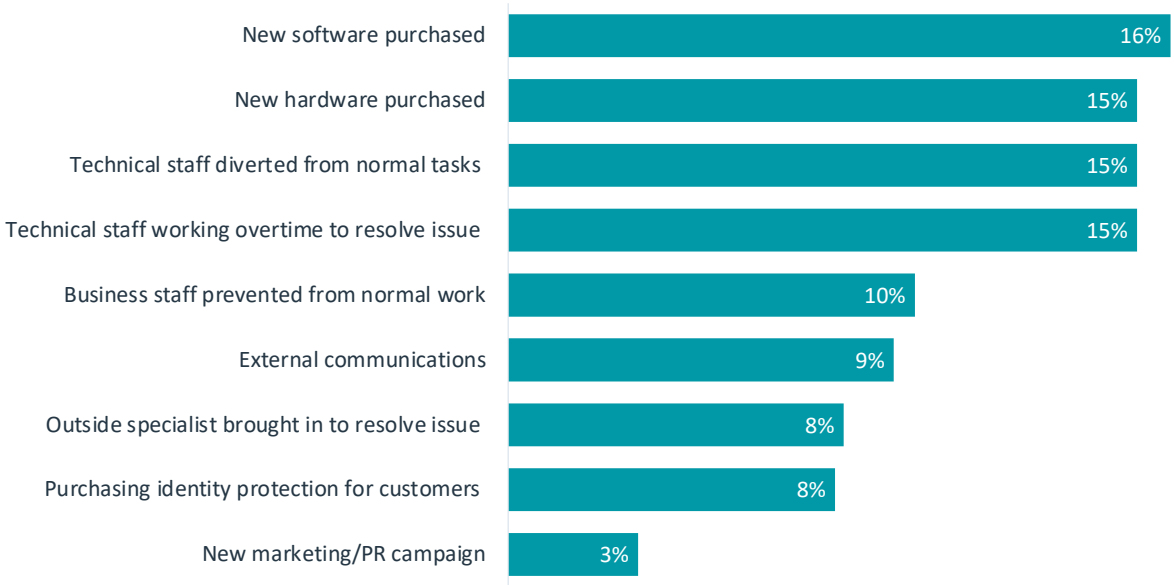
Changes in Approach to Cybersecurity



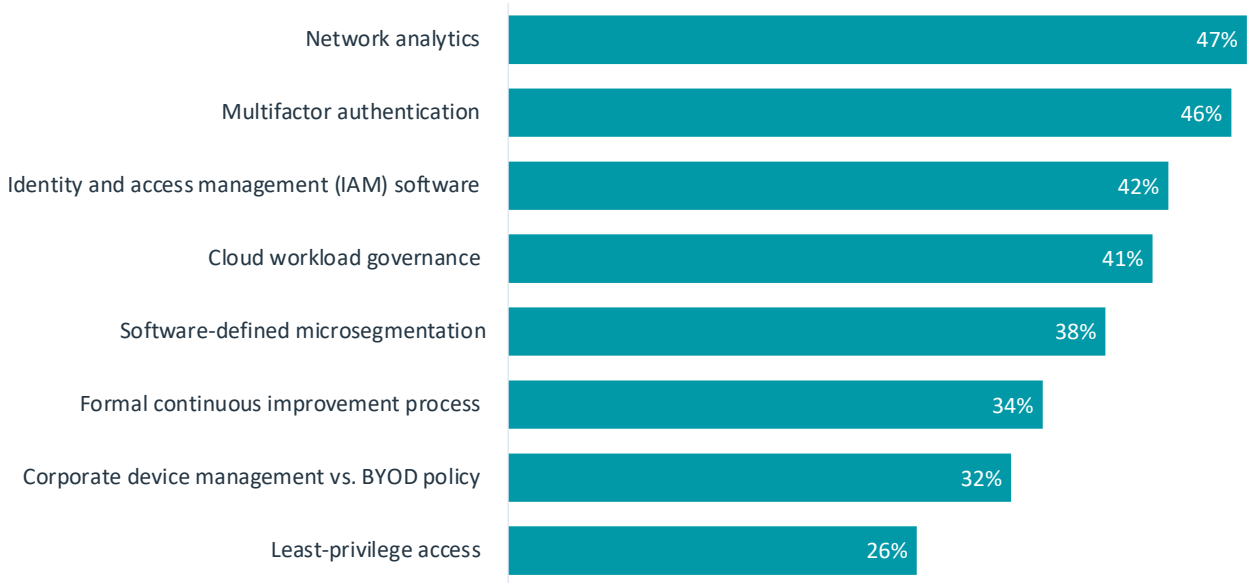
Cybersecurity Incidents from Past Year



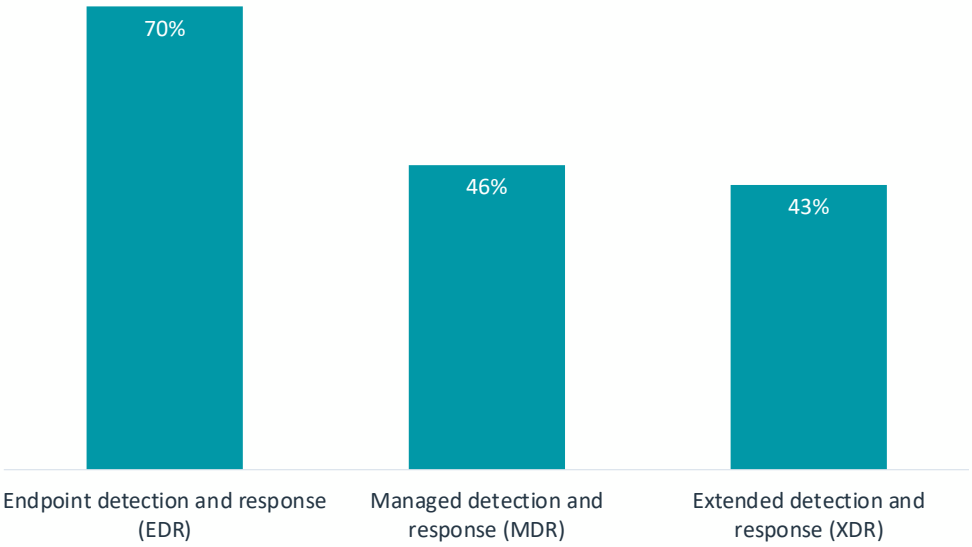
Elements of Incident Mitigation



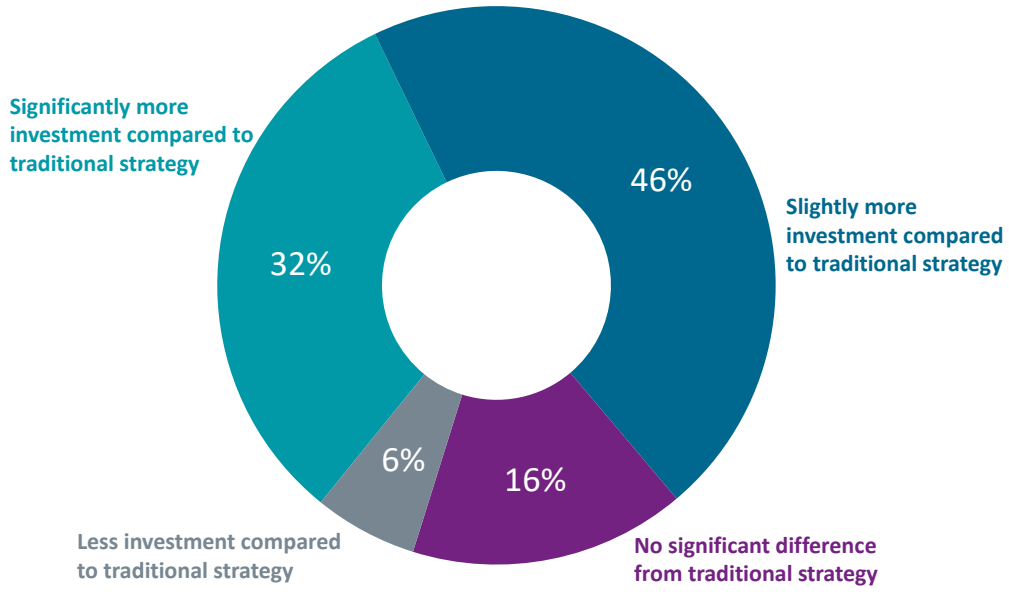
Zero Trust Practices in Place



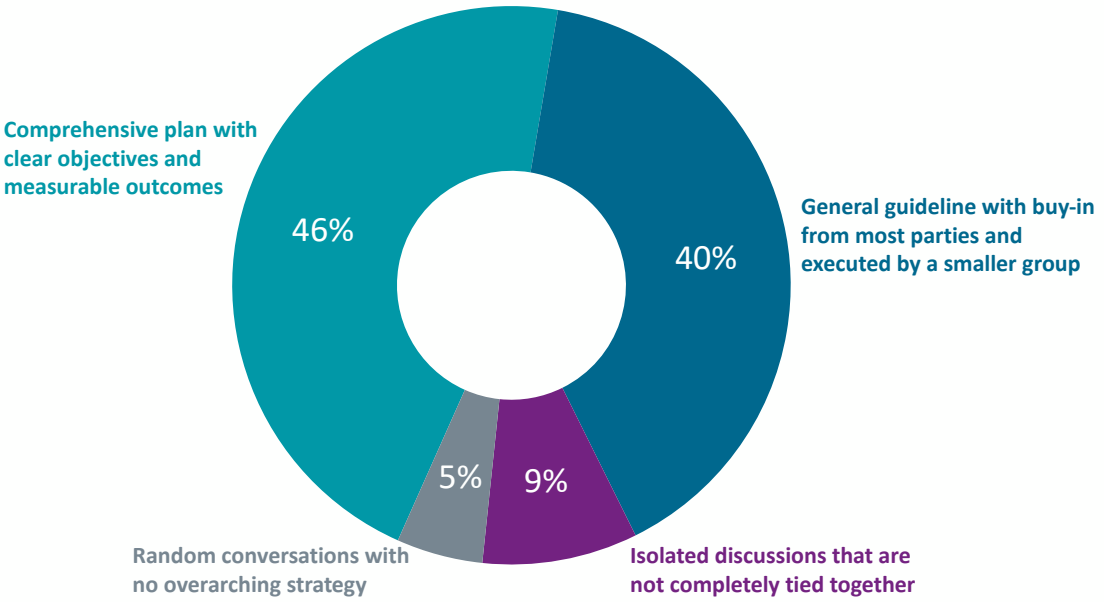
Detection and Response Tools



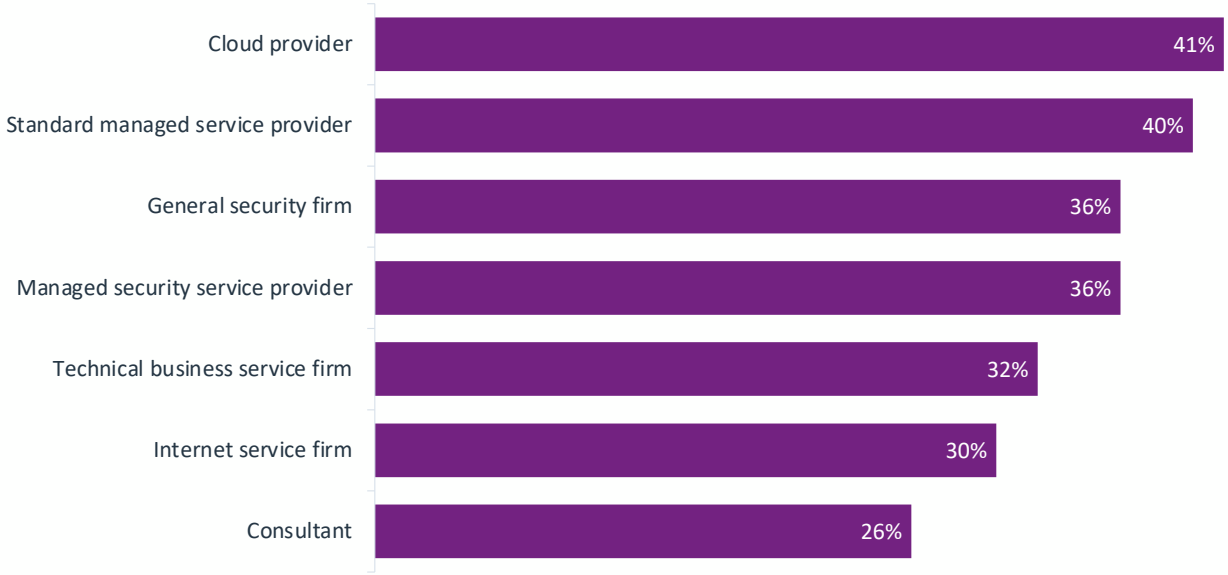
Investment Needed for Zero Trust



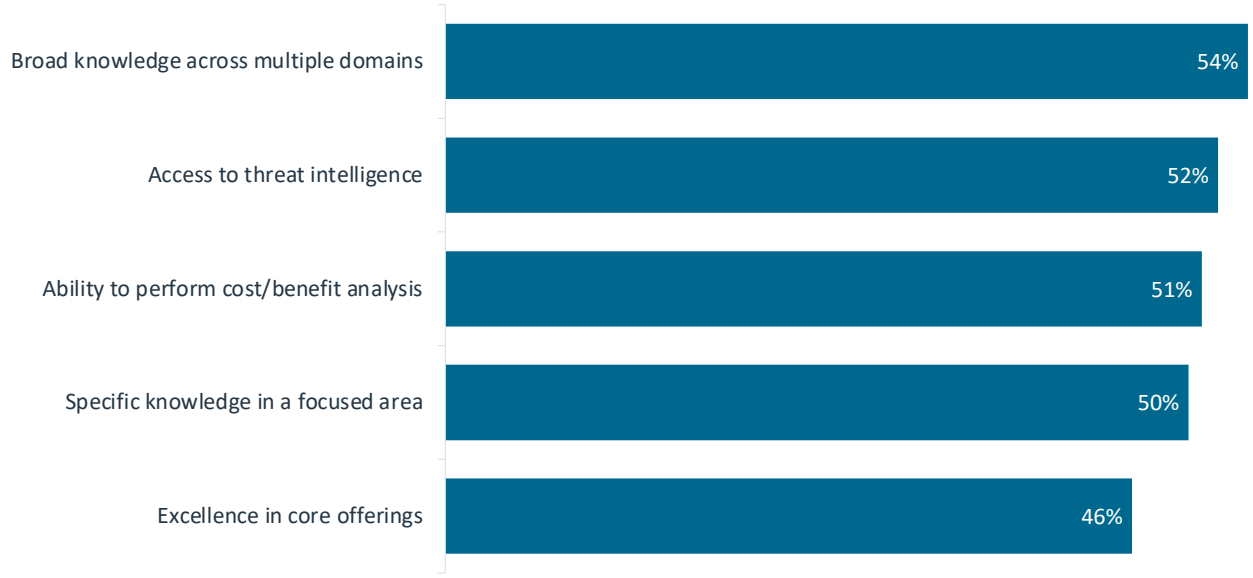
Nature of Discussion in Cybersecurity Chain



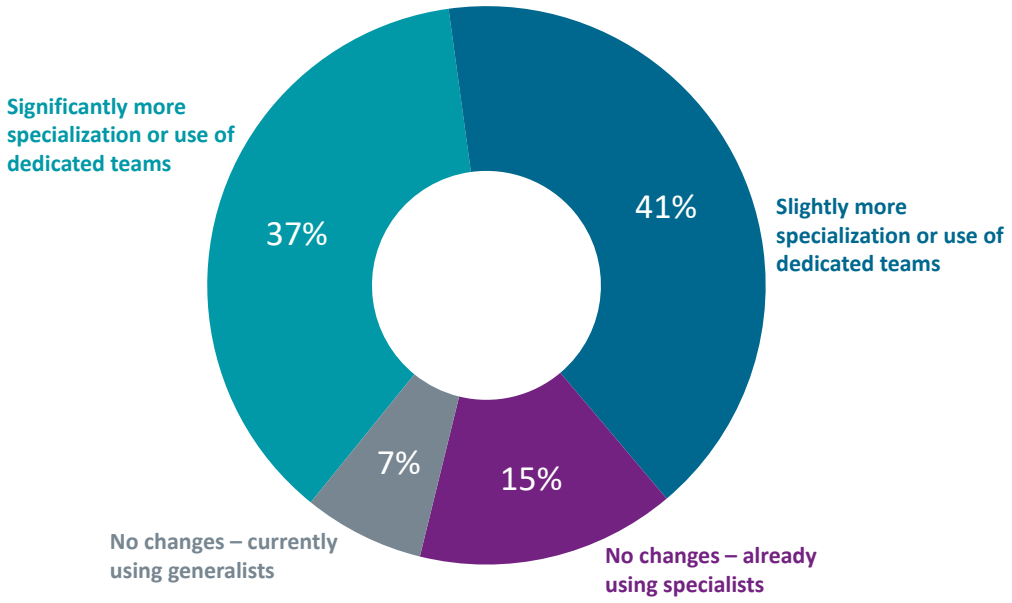
Types of Third-party Firms Involved with Cybersecurity



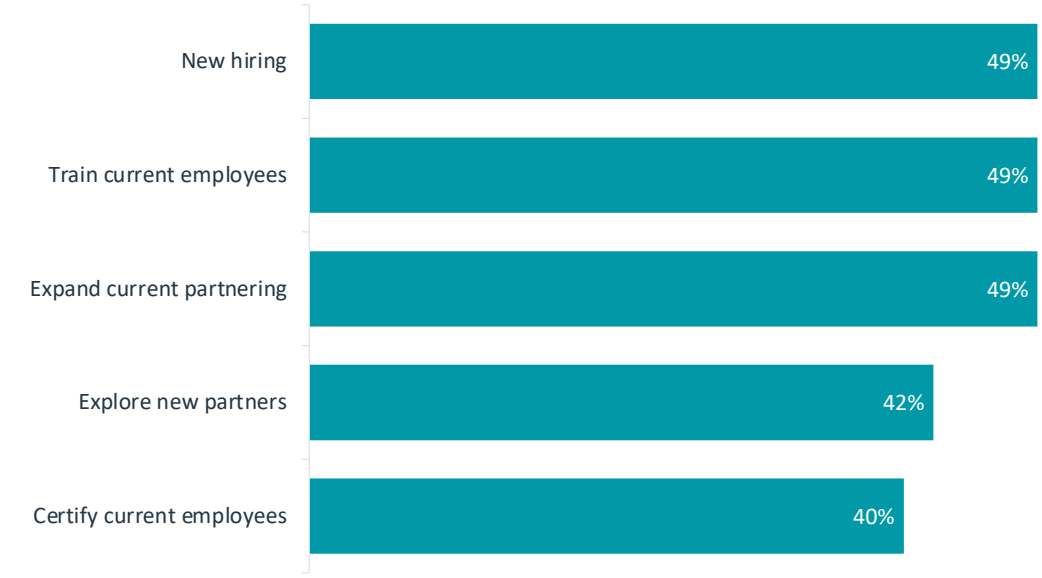
Important Criteria for Third-party Cybersecurity Firms



Approach to Cybersecurity Personnel in Past Two Years

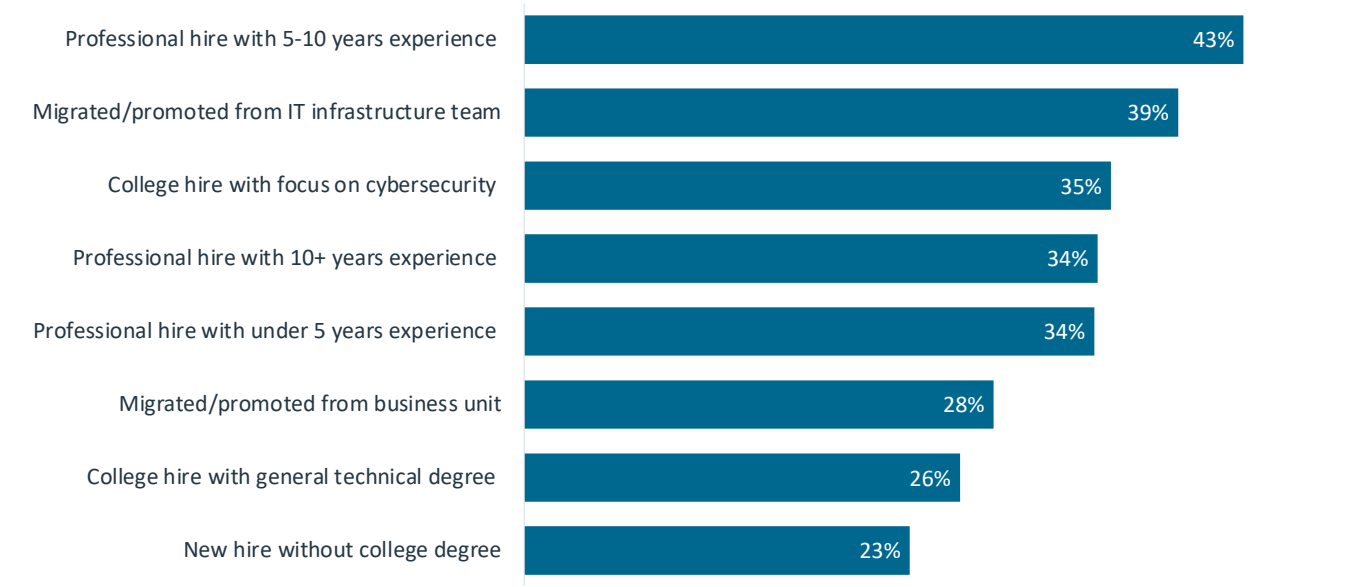


Plans for Improving Cybersecurity Skills



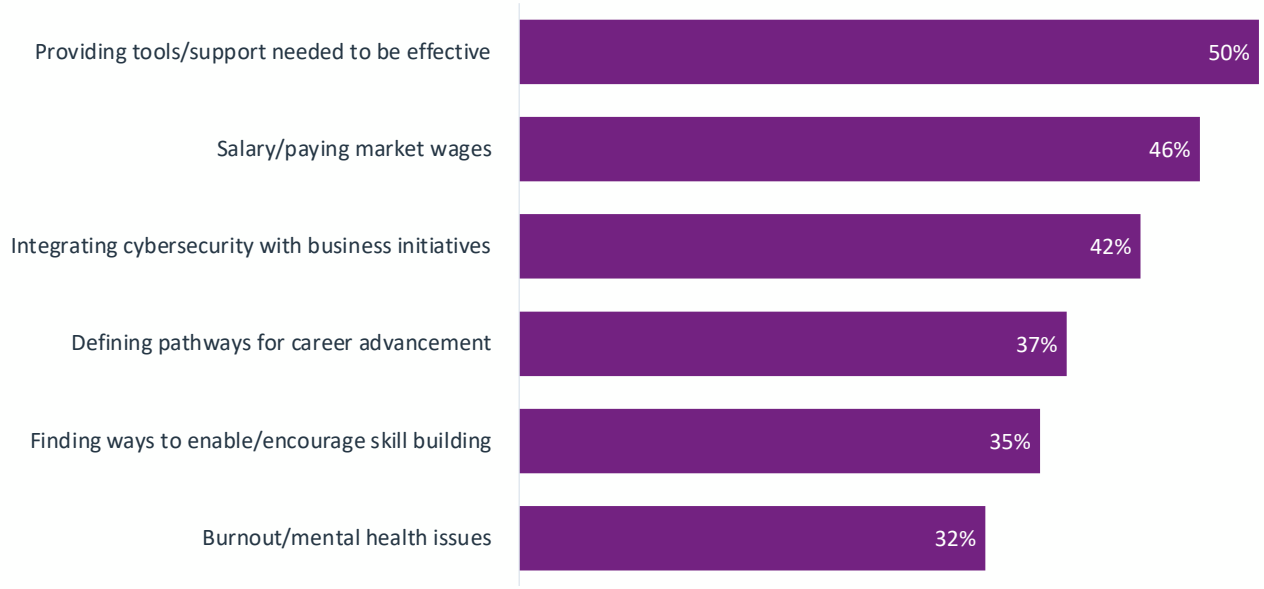
Prerequisite Knowledge for Cybersecurity Roles

Pathways into Cybersecurity Specialization



Potential Steps to Support Cybersecurity Resources

Challenges in Managing Cybersecurity Resources



CompTIA.org

CompTIA is responsible for all content and analysis. Any questions regarding the report should be directed to CompTIA Research and Market Intelligence staff at research@comptia.org.