CompTIA

State of Cybersecurity 2023

Introduction

Cybersecurity is a constant balancing act. For years, the tug-of-war has been framed as a contest between security and convenience. In both business environments and the consumer space, tighter security controls often correspond with a lower degree of convenience, a tradeoff that most end users are hesitant to make. Organizations can force the issue with technology and policy, but this can open the door for risky workarounds.

Today, a new challenge is emerging. For chief information security officers (CISOs), chief information officers (CIOs) and others involved in maintaining corporate security, the conflict is not so much with convenience as it is with progress. As organizations go through digital transformation and tie technology initiatives tighter to business success, excessive cybersecurity measures can hinder overall progress. Of course, cybersecurity measures that are too relaxed can lead to serious incidents, resulting in potentially greater impacts for progress.

CompTIA's 2023 State of Cybersecurity report explores the many variables that must be considered in balancing the cybersecurity equation. As cybersecurity becomes a critical business imperative, every process must be scrutinized for potential vulnerabilities. This practice of risk analysis then drives decisions around workflow, skill-building and technology implementation. With technology trends evolving and attack patterns changing, true equilibrium is impossible to achieve. The balancing act is a full-time job.

Trends to Watch 2023

Policy

Risk management is the driving force behind cybersecurity

Process

Cybersecurity processes drive a wide range of decision-making

People

Talent pipelines get stronger as firms build skill resilience

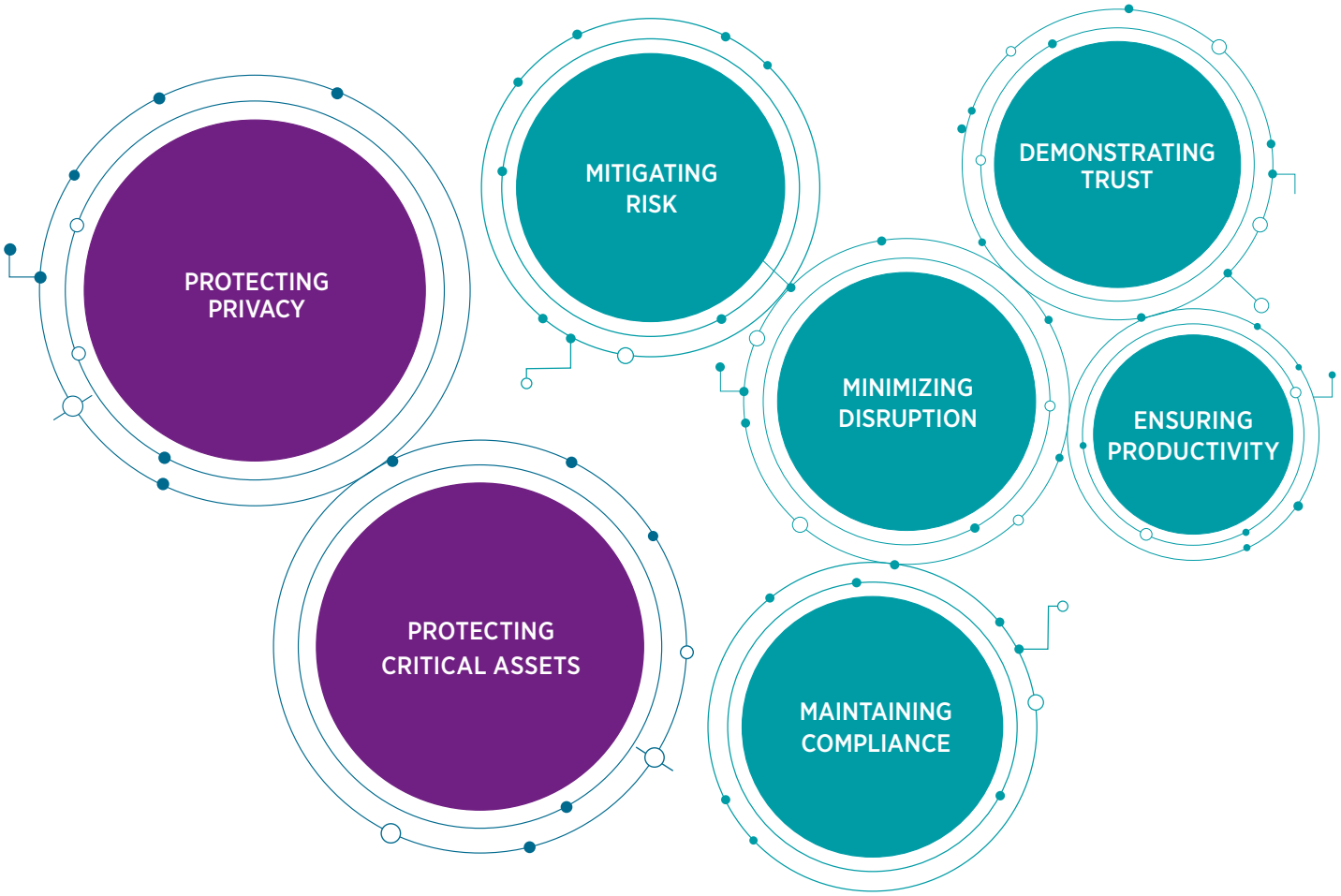
Product

AI drives the cybersecurity product set to new heights

Market Overview

For proof of how difficult it is to find the right balance, look no further than the objectives behind organizational cybersecurity strategies. Six different geographic regions participated in CompTIA's 2023 State of Cybersecurity study, representing a range of economic and technical maturity. Across all six regions, the top priorities for cybersecurity strategies involve the traditional goal of protection, whether that involves protecting critical corporate assets or protecting the privacy of customer data.

Objectives for Cybersecurity



Source: CompTIA 2023 State of Cybersecurity | n=1156 technical and business professionals

Protection is only one piece of the puzzle, though. As operations become more digitized, a robust cybersecurity approach is required for minimizing operational disruption, maintaining compliance with a growing list of regulations or establishing trust as part of the corporate brand. Accomplishing these objectives requires more than just keeping threats on the outside; it requires a proactive mindset around healthy internal processes. For the remainder of this report, the focus is on U.S. data. Separate research briefs highlight data points from international regions.

Many Issues Drive Cybersecurity Concerns

Source: CompTIA 2023 State of Cybersecurity | n=511 U.S. technical and business professionals

The simplest way to describe both the corporate stakes for cybersecurity and the challenges involved in crafting cybersecurity policy is to say that the scale has grown dramatically. From a threat perspective, companies can see that the number of cybercriminals is skyrocketing and their organizational ability is growing. At the same time, the potential damage from an attack can be catastrophic. From a data perspective, there is far more data being captured, with both privacy implications for customers and operational risk for internal workflows. From a product perspective, generative artificial intelligence (AI) is accelerating capabilities, often making the skill gaps at organizations even wider.

One aspect of scale that may be underestimated in the United States is the rise of external drivers for cybersecurity. The most common type of external driver is government regulations. Within any individual country, there are increasingly complicated cybersecurity guidelines, extending beyond typical highly-regulated industries such as healthcare or finance. For organizations operating globally, navigating different country regulations is even more challenging. Other types of external drivers include contractual requirements between businesses entering into a relationship or stipulations that come as part of cyber insurance policies.

Cybersecurity Changes In the Past Year

Source: CompTIA 2023 State of Cybersecurity | n=511 U.S. technical and business professionals

Addressing the big problem of cybersecurity requires a multi-faceted approach. Processes throughout the organization must be improved, especially those relating to incident response. Skill gaps need to shrink, whether that involves broad workforce education, dedicated cybersecurity resources, external partners or (often) a combination of all three. The toolbox has to grow, with targeted technology addressing specific activities and dashboards to pull everything together.

Slowly but surely, these changes in the approach are having an effect. When it comes to the overall state of cybersecurity in the economy, 67% of survey respondents feel that the situation is improving, including 27% that feel the situation is improving dramatically. In 2022, only 25% felt that things were improving dramatically. From an organizational perspective, 76% of respondents feel that their organization's cybersecurity is satisfactory, including 28% that rate things as completely satisfactory. In 2022, only 24% were completely satisfied.

It is interesting to note that there is a significant difference in satisfaction between executives and other workers throughout the organization. More than 4 in 10 executives report being completely satisfied with the cybersecurity at their organization, compared to 25% of IT staff and 21% of business staff. The reason behind this could be on either side of the scale. Executives may be given more leeway with technology, giving them more convenience than other employees. On the other hand, the rank and file staff may be wrestling with details of cybersecurity implementation that are invisible to executives. Either way, the gap in satisfaction points to a need for improved communication on the topic.

Even with small gains in satisfaction, there is still plenty of room for improvement. In recent years, businesses have begun to consider cybersecurity as a critical function, intertwined with technology but standing on its own with metrics related to success. The next stage of maturity involves establishing and refining the operations of this standalone unit, using strategic policy and processes to drive tactical actions around personnel and products.

INCIDENTS AND IMPACT

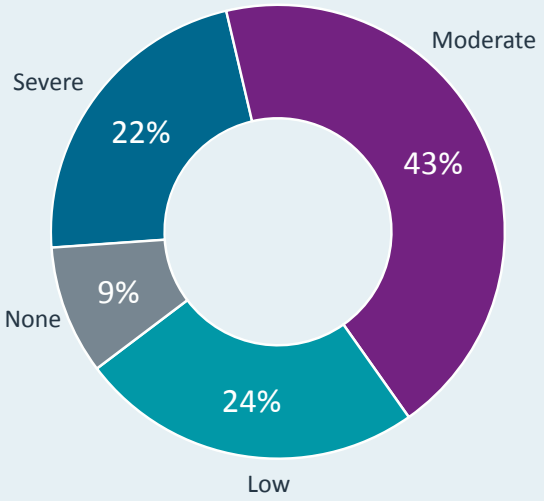
Perhaps the most common query when it comes to cybersecurity is: "What is the cost of a cybersecurity incident?" Answering this question requires two pieces of data from an end user. First, an individual needs awareness that a breach has occurred. Second, they must know the total cost required for mitigation. Neither piece of data is easy to gather.

Recognizing cybersecurity incidents requires both sufficient visibility into systems and agreement on what constitutes an incident. According to Palo Alto Networks' What's Next in Cyber Report, 96% of organizations reported experiencing at least one breach in 2022. In comparison, Splunk's State of Security 2023 report found that 52% of organizations reported a recent data breach, although 87% of orgs reported being targets of ransomware. The wide variety of responses suggests uncertainty around incidents, likely exacerbated by reports of network intrusion going undetected for months.

As for the cost, there are many estimates for the financial impact of cybersecurity incidents. Most notable is IBM's Cost of a Data Breach report, which pegs the global average cost of data breach in 2023 at $4.45 million. This number and others like it attempt to quantify a variety of mitigation efforts, but the final number is skewed due to large enterprise and falls short of detailing the steps that companies should build into a plan.

Mitigating Cybersecurity Incidents in the Past Year

Estimated Impact of Incidents



Common Mitigation Steps

1. Technical staff working overtime
2. Purchase new software
3. Technical staff diverted from routine
4. Employee discipline/removal
5. Purchase new hardware
6. Business staff prevented from workflow
7. External communication plan

Source: CompTIA 2023 State of Cybersecurity | n=511 U.S. technical and business professionals

CompTIA's approach is to ask respondents to gauge the impact of incidents, which normalizes across company size—a $1 million dollar mitigation may be a severe impact for a small firm but a low impact for a giant company. Then respondents are asked to describe the typical steps taken to address incidents. This captures actions that may involve time and effort but do not necessarily show up as a direct cost. For example, one of the top steps described by respondents is discipline or removal of an employee who contributed to the incident, underlining the threat of human error or malfeasance in cybersecurity issues.

1 POLICY:

Risk management is the driving force behind cybersecurity

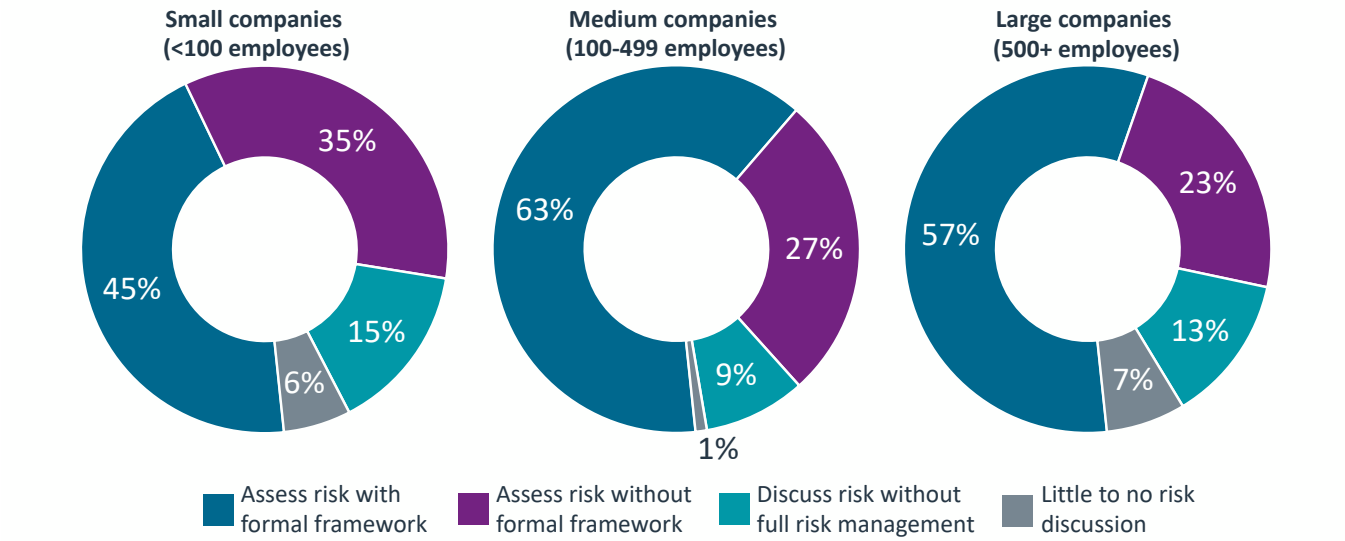
Over the past few years, risk management has been viewed as a component of cybersecurity, growing in importance but existing alongside other tactics as organizations built their overarching mindset. However, risk management is becoming the primary method for solving one of modern cybersecurity's greatest challenges: The connection between cybersecurity efforts and business operations.

This question of cybersecurity metrics has also grown in importance over the past few years. As businesses shifted away from a purely defensive paradigm, they explored new ways to measure the effectiveness of cybersecurity activity. For starters, simply looking backwards to check the number of incidents became insufficient as attacks became harder to detect. More and more, companies were finding that malicious actors had been inside their networks for lengthy periods of time. Beyond that, cybersecurity investments were rising thanks to increased technology adoption and proactive cybersecurity measures.

While enterprise technology in general was embracing return-on-investment calculations during a transition from a tactical cost center to a strategic endeavor, the same calculations usually did not apply to cybersecurity. Cybersecurity is not a direct revenue-generating activity, so there was no return to be gained from additional spending. Instead, metrics such as percentage of systems patched or percentage of workforce trained sought to quantify cybersecurity efforts while other metrics such as mean time between failures (MTBF) or mean time to repair (MTTR) measured architectural resiliency.

These types of metrics provided more rigor into cybersecurity operations, but still left a disconnect between cybersecurity and organizational health. Enter risk management. By identifying various risks, assigning probability of occurrence and potential cost, and proposing mitigation plans, cybersecurity professionals can strengthen the link between cybersecurity spending and desired outcomes. Most companies today understand that there is no such thing as perfect cybersecurity. Rather than being a justification for unlimited spending, though, that reality becomes a driver for rigorous risk management.

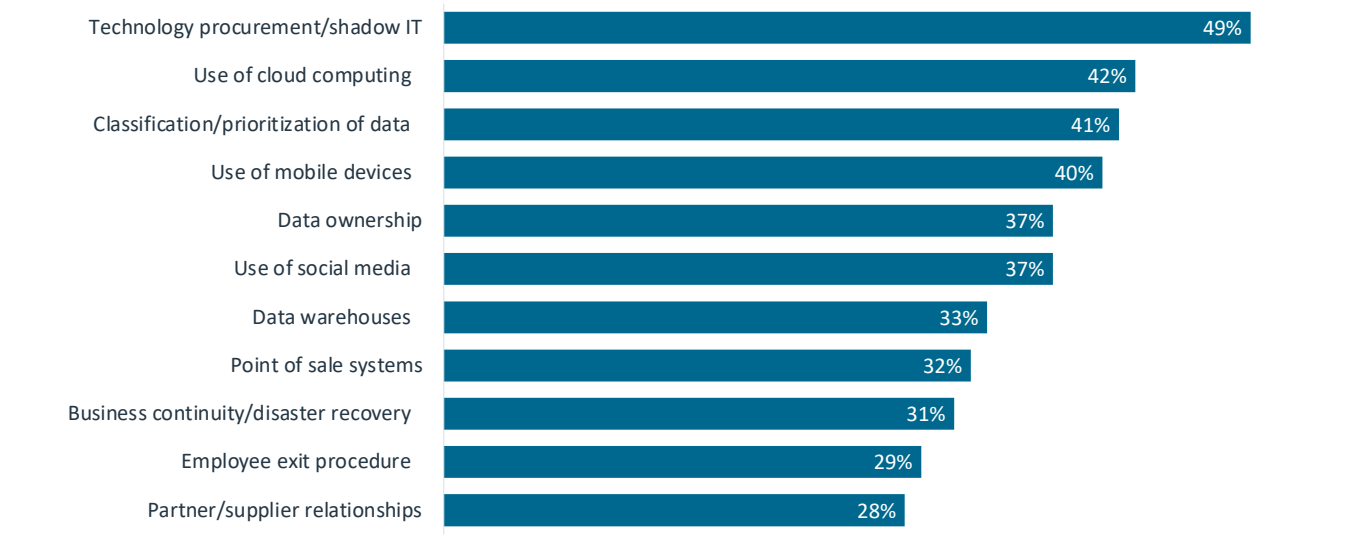
Organizational Approaches to Risk Management



Source: CompTIA 2023 State of Cybersecurity | n=511 U.S. technical and business professionals

The overwhelming majority of companies in CompTIA's survey have at least some discussions around risk management. In some cases, these discussions basically serve to raise the level of awareness, possibly helping smooth over minor disagreements around cybersecurity initiatives. Nearly 30% of companies take a more serious approach, assessing risks throughout the organization but not using a formal risk management framework. Just over half the firms surveyed take a leading approach, using a framework such as the NIST Risk Management Framework (RMF) or the IRGC Risk Governance Framework to identify and manage risks and related spending.

Topics Included in Risk Analysis



Source: CompTIA 2023 State of Cybersecurity | n=488 U.S. technical and business professionals

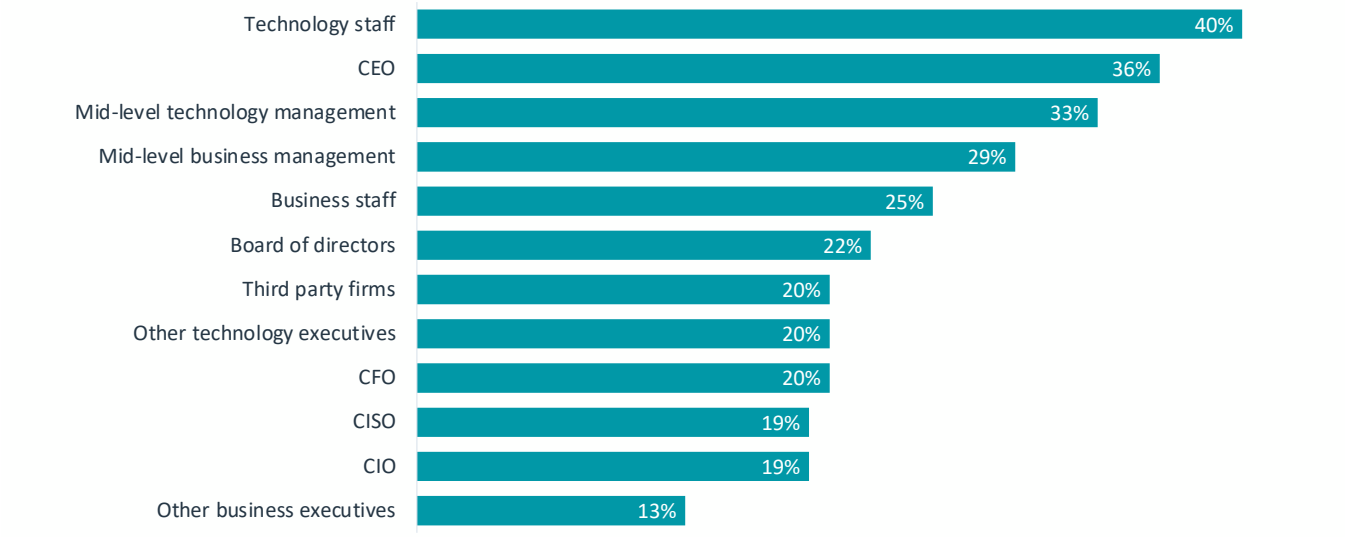
One of the best reasons to use a formal framework is to help identify areas that may lie outside traditional IT system architecture. Among the sampling of topics presented in CompTIA's survey, there is healthy adoption across a wide range of interests. Leading the pack is risk analysis related to technology procurement. This is another example of a balancing act—giving more leeway to business units to find and use suitable technology will increase efficiency, but the primary downside of shadow IT is that business units lack the necessary cybersecurity skills to properly secure the systems they are choosing.

Cloud computing, data classification/ownership and the use of mobile devices are all areas of risk analysis more closely aligned with typical IT activity. There are clear front-end benefits to these initiatives, such as feature-rich software as a service, insightful data analysis and a high degree of accessibility. However, those benefits must be assessed against risks such as system sprawl, data silos and mismanagement by users.

Beyond technical topics, thorough risk analysis also examines policies and processes that may have little to do with the IT team. When it comes to social media, companies have no ownership over the systems where employees may be posting their own pictures and comments. In an era of social engineering, though, there must be precise guidelines around the content being shared since it could eventually lead to a breach. Likewise, employee exit procedures must be carefully considered, especially as remote work lowers the opportunity for oversight following a termination.

Finally, business relationships should be part of risk analysis. While this area ranks lowest among respondents in CompTIA's survey, relationships with other firms inevitably involve some form of data sharing, if not outright access to other systems. The chain of digital operations is only as strong as its weakest link, and when that chain involves outside parties, finding the weak link requires detailed planning.

People Involved in Risk Management Discussions



Source: CompTIA 2023 State of Cybersecurity | n=488 U.S. technical and business professionals

Along those same lines, companies have internal chains of cybersecurity responsibility. Making these chains as strong as possible involves including many different individuals in risk management discussions, according to their role in various risks. It is no surprise to see technology staff leading the list of participants in risk discussions. It is somewhat of a pleasant surprise to see the CEO listed second. Ultimately, these decisions are business decisions instead of technology decisions, and the CEO has the responsibility of weighing all the information and making the final call.

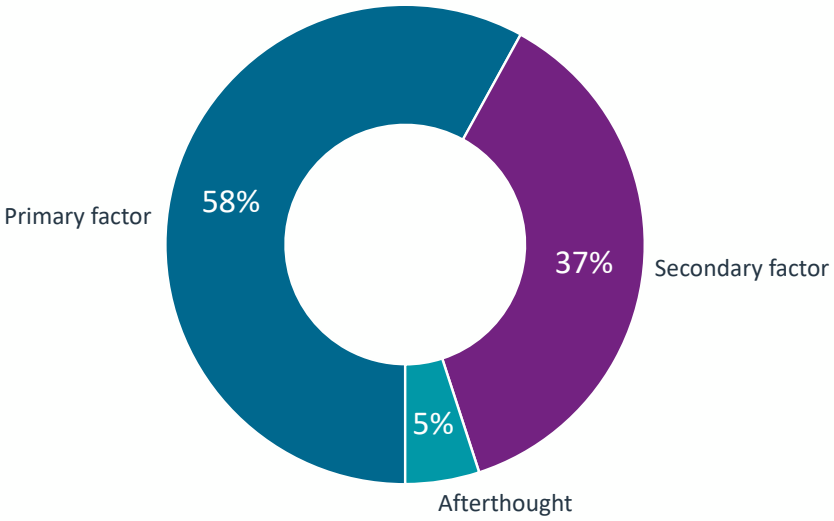
Unfortunately, business involvement drops after that. More companies should consider including a wide range of business professionals, from executives to mid-level management to staff positions, in risk management discussions. The reason why goes back to the leading topic of risk analysis. These individuals are becoming more involved in technology decisions for their departments, and without a proper view into the associated risks, their decisions may have harmful consequences.

In its State of Cybersecurity Resilience 2023 report, Accenture identifies a group they term "cyber transformers." These organizations "not only embed three key cybersecurity actions into their transformation efforts but also apply strong cybersecurity operational practices from the start." What is the first of the three key cybersecurity actions? The integration of cybersecurity and risk management. Risk management is no longer a nice-to-have. It is the defining methodology for modern cybersecurity.

2 PROCESS:
Cybersecurity processes drive a wide range of decision-making

Building policy is largely a cultural and philosophical exercise that sets the agenda and guidelines for cybersecurity tactics. Establishing and executing the correct processes is the first part of that tactical work. For many companies, considering the overarching policy and instituting secure processes may feel like unnatural first steps in building a secure posture, which was historically done through technology. The nature of modern business with deeply integrated technology mandates much more of a top-down approach.

As organizations place more emphasis on the process piece of the cybersecurity puzzle, they are discovering that the influence of cybersecurity extends far beyond direct questions of security implementation. Following a comprehensive risk management discipline, both building cybersecurity processes and integrating cybersecurity into business workflows drives many functional decisions.



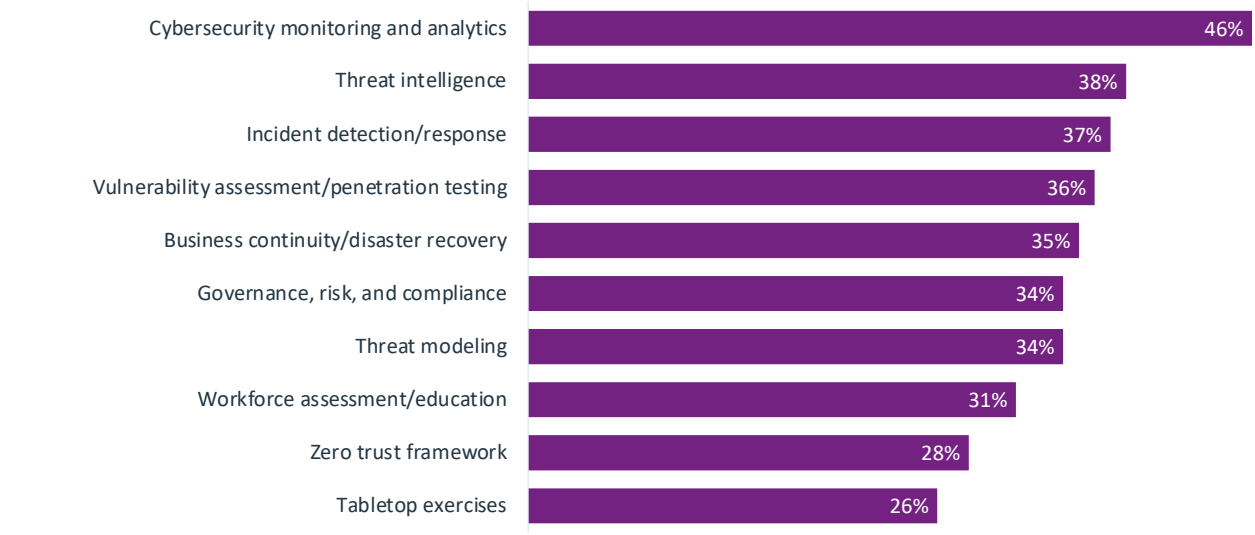
Source: CompTIA 2023 State of Cybersecurity | n=511 U.S. technical and business professionals

First and foremost, cybersecurity is becoming a primary factor when evaluating new technology. One challenge for many cybersecurity professionals, especially in the past decade, has been playing catch-up as new technology is adopted for digital transformation. The appetite for accelerating tech adoption has grown as companies seek to use technology for strategic advantage, and cybersecurity concerns have not always been top of mind when pursuing new technology initiatives.

Companies in CompTIA's survey report pursuing a variety of different initiatives spanning different technology disciplines, from infrastructure (ongoing migration to cloud architecture) to software (improving web/mobile presence) to data (implementing data management or database administration). Any one of these initiatives would be a major project on its own; often, companies are combining initiatives to pursue a new business objective.

This complex scenario is ripe for creating new vulnerabilities. It is heartening to see that 58% of companies view cybersecurity as a main consideration when assessing new initiatives, but too many firms are still treating cybersecurity as a secondary factor or even an afterthought. Especially as technology adoption is happening with less oversight from a traditional IT department, organizations must ensure that cybersecurity is front and center in any discussion of new systems.

Elements of Organizational Cybersecurity Strategy



Source: CompTIA 2023 State of Cybersecurity | n=511 U.S. technical and business professionals

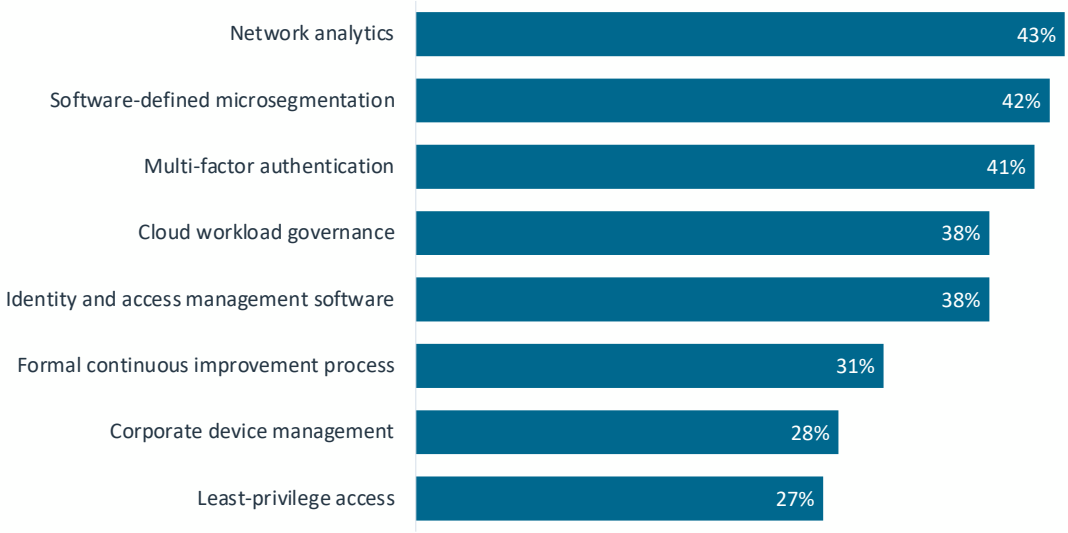
Beyond technology implementation, other elements of cybersecurity strategy point to the impact cybersecurity is having on other business activities. For example, threat intelligence is no longer just about viruses or malware. New types of threats such as social engineering and ransomware highlight the intersection of technology systems and real-life circumstances. As mentioned previously, a strong social media policy for employees not only ensures consistent brand positioning but also guards against sharing information that could be used in a social engineering attack. Similarly, comprehensive policies around data management and backups can mitigate the risk of ransomware.

Another example is governance, risk and compliance (GRC). In the past, this specialization has largely applied within highly regulated industries. Today, the complex web of regulations governing digital business is driving every organization, regardless of size or industry, to become much more cognizant of how they conduct business. As with best practices in cybersecurity, best practices in GRC must be communicated throughout the workforce, ideally tailored to job function.

This leads to a final process example of workforce education. The responsibility of the individual employee for maintaining secure practices has never been higher. As remote and hybrid work continue to redefine the way employees operate, companies must reassess policies (and enforcement) around device management, information sharing and communication tools. These policies cannot be created in a vacuum by HR. Cybersecurity professionals must be part of the collaboration, offering their expertise to processes owned by someone else.

The general intent of any cybersecurity process, whether direct or indirect, is to align with the principles of a zero trust framework. At a high level, a zero trust framework is simple to define—it means adding a layer of verification to any transaction rather than only trusting in the individual components. In practice, the details get more complicated. Many companies may assume that a zero trust framework involves a specific set of products or a single methodology. The reality is that there are many actions that fall under the zero trust umbrella.

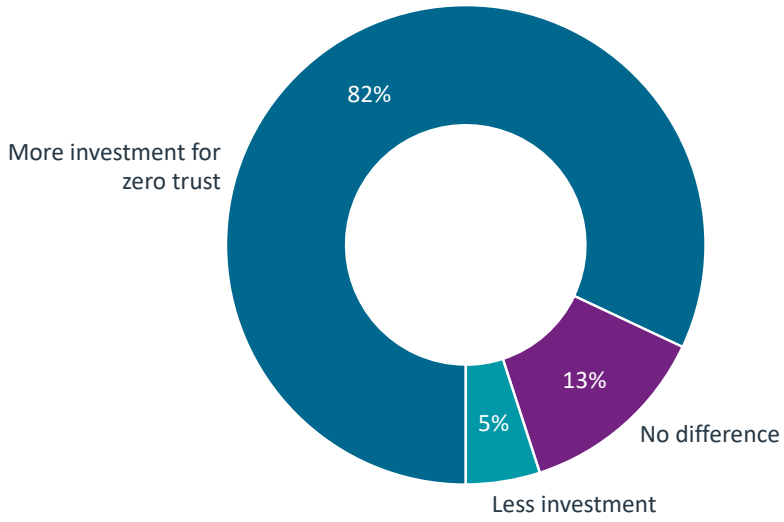
Practices Included in Cybersecurity Strategy



Source: CompTIA 2023 State of Cybersecurity | n=511 U.S. technical and business professionals

Although only 28% of firms in CompTIA's study identify a zero trust framework as part of their cybersecurity strategy, there are more firms following individual practices that are commonly included in a zero trust approach. Practices such as software-defined microsegmentation or multi-factor authentication predate the rise of the zero trust buzzword, but the underlying goal is the same: Eliminating any activity that cannot be isolated or independently verified.

Zero Trust Framework Investment vs Prior Cybersecurity Investment



Source: CompTIA 2023 State of Cybersecurity | n=511 U.S. technical and business professionals

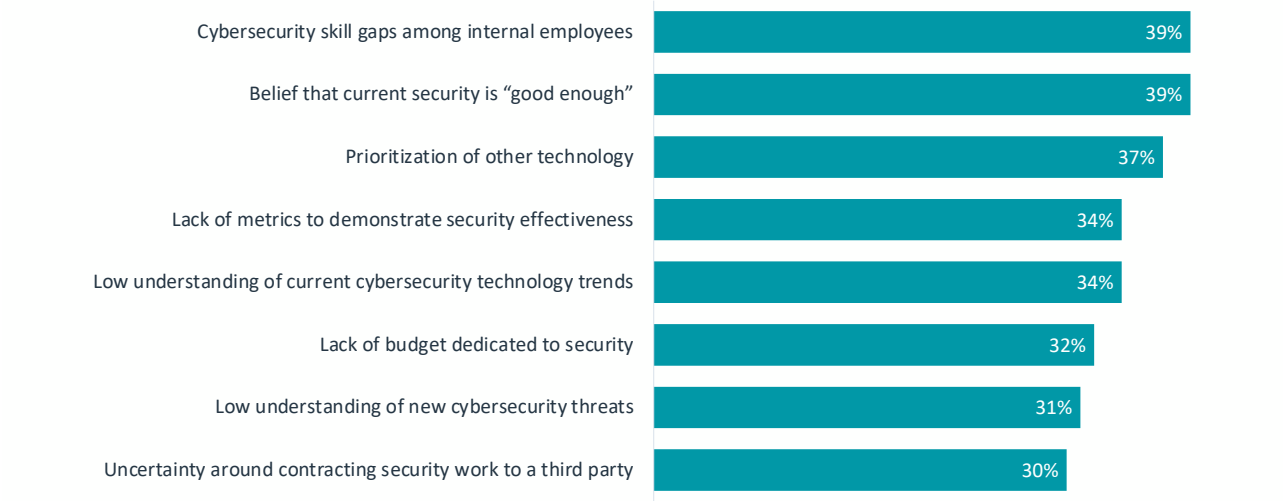
For those who recognize a zero trust approach within their organization, the budget implications are likely a reflection of what all firms are facing when it comes to cybersecurity. As expected, adding layers of verification comes at a higher cost. Presumably, integrating cybersecurity with a wide range of business activity also comes at a higher cost. To the chagrin of finance departments, the exact cost may be difficult to capture. Not every individual with cybersecurity expertise is a standalone cybersecurity professional, and not every technology contributing to a secure posture is a standalone cybersecurity tool.

Still, organizations are feeling the cybersecurity budget swell, whether that is in money spent or in time allocated to updating processes. This ties back to the risk management mindset. Although it may not be easy to move away from thinking of cybersecurity as a cost center and there may be no way to directly correlate cybersecurity with revenue, ultimately there needs to be some justification for increased spending. Lower risk is a justification that most executives and boards will understand.

3 PEOPLE:
Talent pipelines get stronger as firms build skill resilience

Organizations are clearly recognizing the importance of cybersecurity skills across their workforce. CompTIA's Cyberseek tool shows that there were over 660,000 cybersecurity-related job openings in the United States between May 2022 and April 2023, representing a 28% increase from the same time period in 2020. Not all of these job postings are for dedicated cybersecurity positions, but they are all technical roles that require some depth of cybersecurity expertise. The number of non-technical workers requiring a functional awareness of cybersecurity practices for their job would stretch even higher.

Challenges to Cybersecurity Initiatives

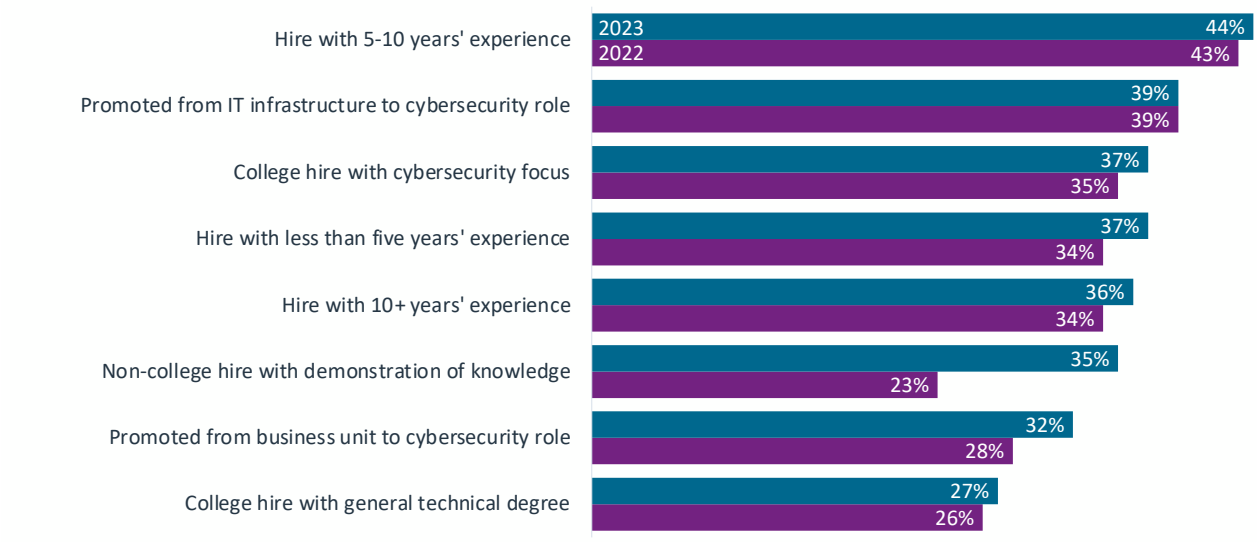


Source: CompTIA 2023 State of Cybersecurity | n=511 U.S. technical and business professionals

This year marks the first time that the top cybersecurity challenge cited by respondents to the State of Cybersecurity study is something other than the general belief that current measures are "good enough." By a slim margin, the top challenge is now cybersecurity skill gaps. This is a significant development; the viewpoint that cybersecurity measures are adequate may not be based on specific data, and acknowledging skill gaps is a shift toward recognizing that there simply may not be enough expertise to even make a qualified assessment.

Recent years have seen a steady progression towards specialization, with companies establishing teams of dedicated cybersecurity professionals rather than relying on IT generalists with cybersecurity as just one part of the overall job description. Typically, these efforts have focused on bringing in mid- to late-career employees who can hit the ground running as they implement best practices. That practice may still be a top choice, but it is not the best method for long-term construction of a deep cybersecurity team.

Pathways for Dedicated Cybersecurity Personnel



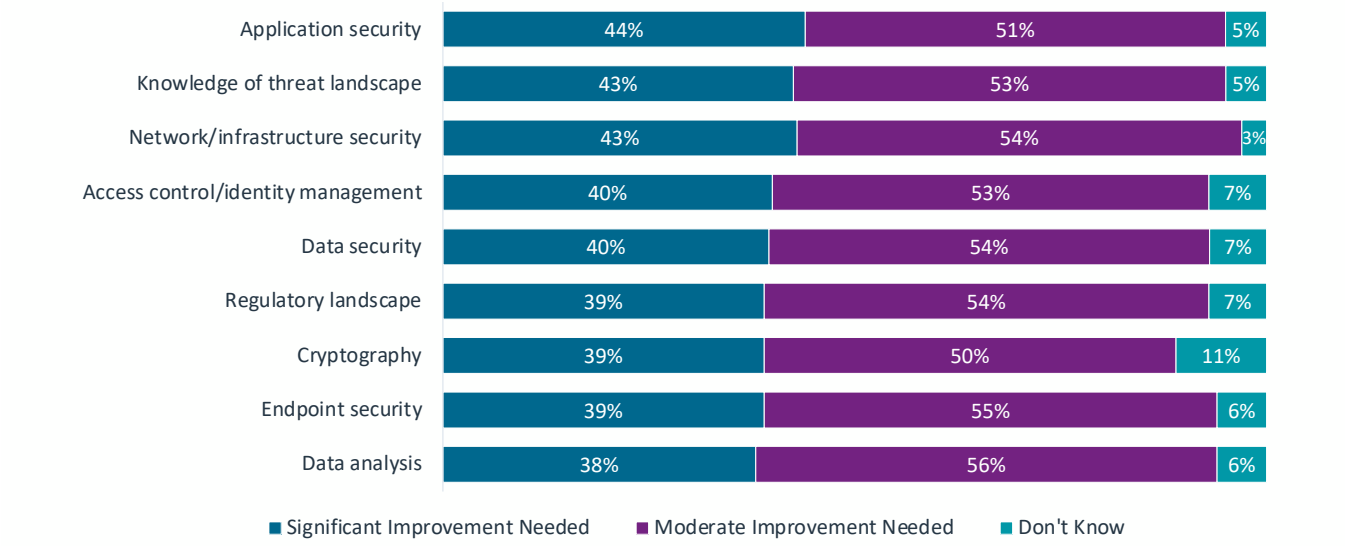
Source: CompTIA 2023 State of Cybersecurity | n=250 U.S. technical and business professionals with hiring plans
CompTIA 2022 State of Cybersecurity | n=309 U.S. technical and business professionals with hiring plans

Instead, companies are turning toward methods that will bring in less experienced cybersecurity professionals who can then continue building their skills while also becoming familiar with corporate culture and objectives. Many of the team-building options that grew in popularity between 2022 and 2023 were those options focused on newer employees, such as college hires or those with less than five years of experience.

The hiring pathway with the greatest year-over-year change was the intent to hire individuals that may not have a relevant college degree (or any college degree at all) but are able to demonstrate subject matter expertise via certifications or other credentials. Many trends in enterprise technology, including the specialized focus on cybersecurity, are evolving faster than traditional learning pathways can keep up with. This is driving employers to look for different avenues for candidates to prove their knowledge, which also has the effect of broadening the candidate pool and improving diversity within the workforce.

Regardless of the hiring pathway, there are bound to be some skill gaps that remain when new individuals are brought into an organization or when internal employees transition to cybersecurity from a previous job responsibility. As a result, businesses continue turning to internal training as the primary avenue for closing skill gaps. Half of the survey respondents use internal training to improve cybersecurity skills, with 43% taking the additional step of helping employees pursue certifications to validate the knowledge.

Areas of Improvement for Cybersecurity Personnel



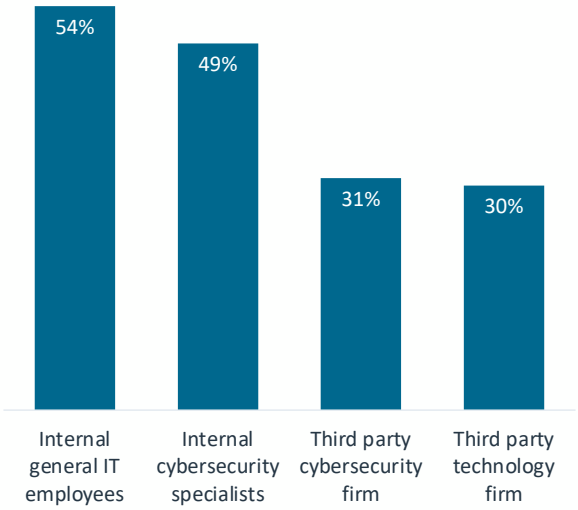
Source: CompTIA 2023 State of Cybersecurity | n=511 U.S. technical and business professionals

In terms of topics for the training, there is no shortage of fields where companies would like to see improvement. As in previous years, the desire for improvement may not obviously align with the self-assessment of current skills. While 44% of companies believe significant improvement is needed in application security, 42% of companies believe they already have expert-level skills in this area. The demand for improved skills may come from firms who view their current skills as relatively low, or it may come from firms who view their current skills as relatively strong but recognize a constant need for learning the latest trends in a fast-changing field.

In addition, the overlap between skill assessment and desire for improvement may point to a need for improving the methodology for assessing skills. Especially since cybersecurity itself is a relatively new specialization for many companies, the many facets within cybersecurity likely represent unfamiliar areas. Developing a regular skill assessment regimen based on industry expertise and best practices is a key step in understanding the exact nature of the gaps that need to be filled.

Making the situation even more complicated, the skills required for robust cybersecurity operations extend beyond the skills that directly address specific components of cybersecurity. The complex nature of modern IT architecture and the need for constant monitoring drive demand for automation, which can extend the capabilities of a cybersecurity team by handling routine tasks and freeing up resources for strategic planning. As AI and machine learning (ML) become more prominent parts of a cybersecurity workflow, there will also need to be commensurate upskilling in the practice of using these technologies and understanding the outputs they produce.

Groups Involved in Cybersecurity Initiatives



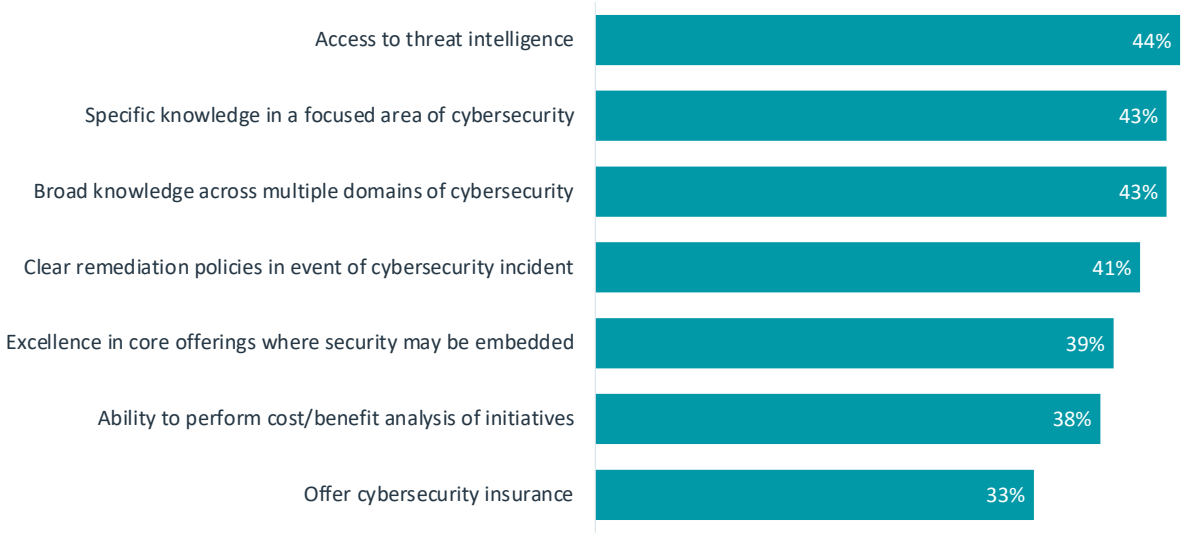
Types of third parties used

1. Managed service provider with many core IT offerings
2. Managed service provider exclusively focused on cybersecurity
3. General security firm offering both cybersecurity and physical security
4. Firm providing technical business services
5. Cloud providers with security embedded into offerings

Source: CompTIA 2023 State of Cybersecurity | n=511 U.S. technical and business professionals
n=314 U.S. technical and business professionals using third parties for cybersecurity strategy

Given the wide array of skills needed for a strong cybersecurity posture, many firms are turning to third parties to assist with cybersecurity strategy. Nearly one third of companies surveyed use third-party firms with a dedicated cybersecurity practice, and approximately the same number use third-party firms that provide a variety of technology services. There obviously may be overlap between these two, as companies use a variety of partners and technology providers to build their overall technology footprint and to complement internal resources.

Criteria Used in Selecting Third-Party Firms



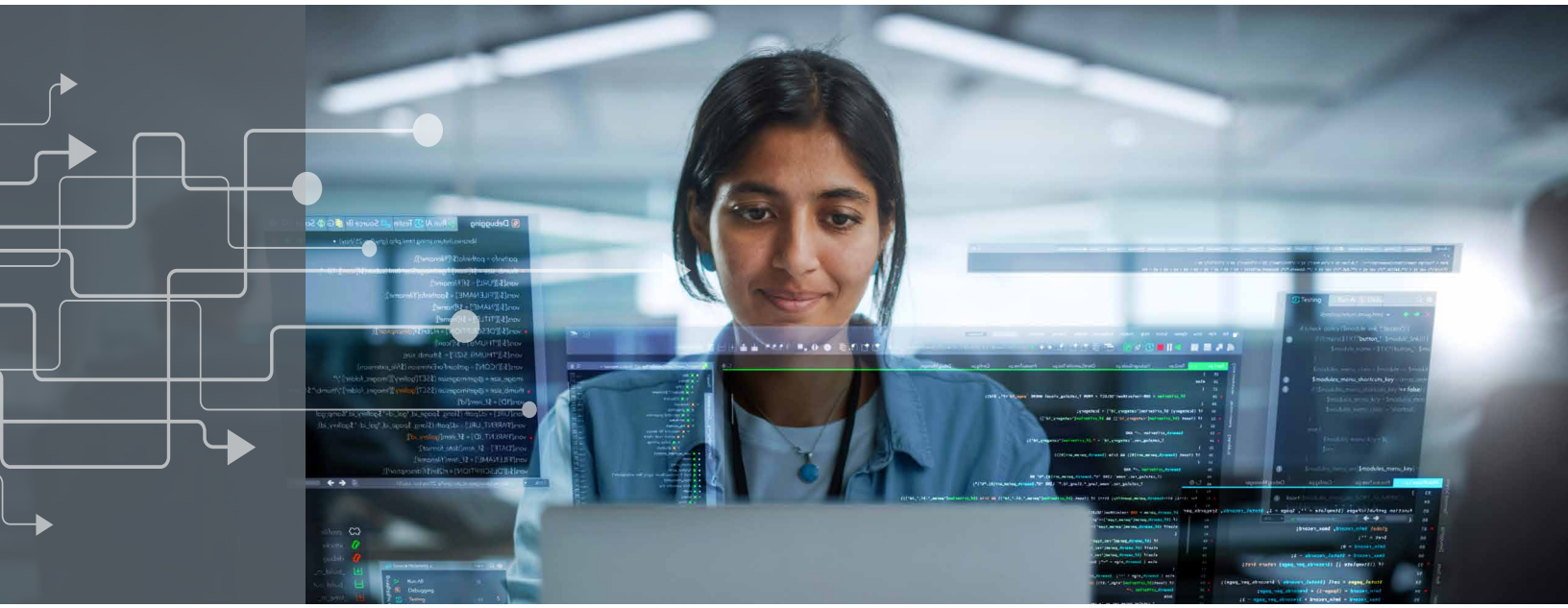
Source: CompTIA 2023 State of Cybersecurity | n=314 U.S. technical and business professionals using third parties for cybersecurity strategy

When it comes to selecting third-party firms or assessing their capabilities in the area of cybersecurity, organizations have clearly learned from the early days of cloud computing. During initial cloud adoption, many companies made assumptions about the level of cybersecurity being provided by their cloud vendor. This created vulnerabilities as applications were migrated from a secure environment to a cloud system where only the infrastructure might be secured but not the application itself or the data being transmitted.

Today, organizations are taking a much more comprehensive approach to selecting vendors or partners. First and foremost, end users are looking for outside firms who understand the modern threat landscape and have access to threat intelligence. This access may come from proprietary investigation done by the third party or by the third party being part of a peer network or information sharing and analysis organization (ISAO).

Beyond threat intelligence, the criteria may depend on the situation, whether the end user is looking for general help building a cybersecurity strategy or looking for specific help with a single focus area. Finally, the issue of liability is on everyone's mind, as there needs to be clear lines of demarcation and responsibility in the event of a security incident or data breach. End users may be looking for agreements or pricing based on outcomes, but providers need to be careful in building arrangements that require certain behavior on the part of the customer.

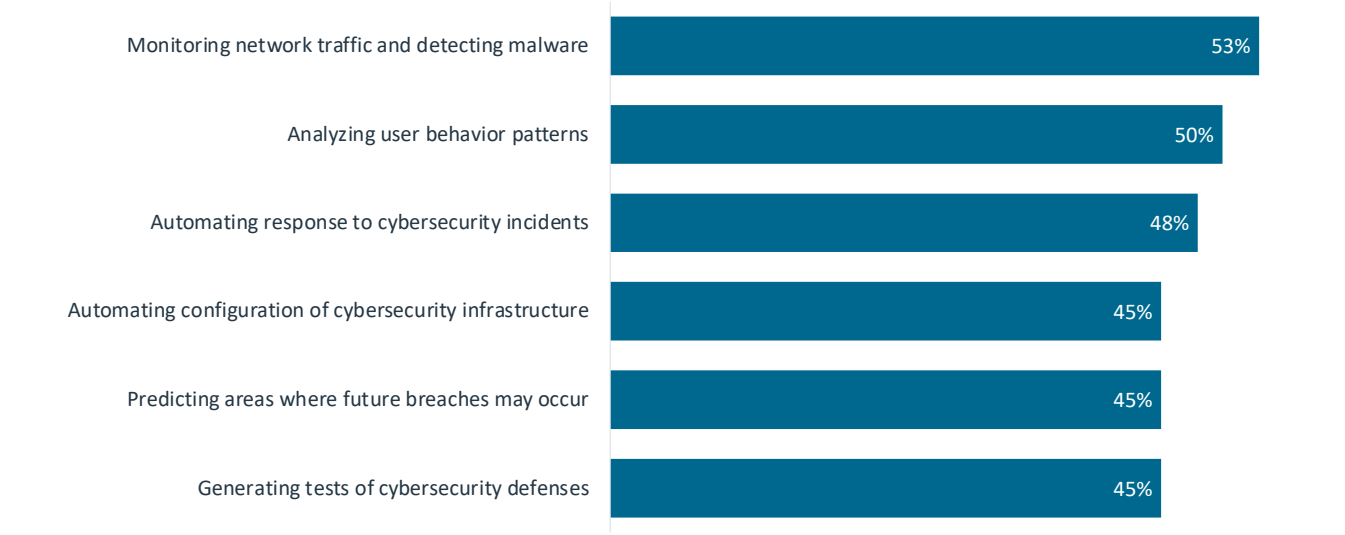
4 Product:
AI drives the cybersecurity product set to new heights



By a large margin, the technology trend capturing the attention of both IT teams and business leaders has been generative AI. In fact, many believe that this new wave of AI, based on large language models (LLMs), is the biggest tech paradigm shift in decades. The possibilities are exciting, but as with most trends the situation is more complicated than simply delivering overnight success.

For background, generative AI should be viewed as a step forward in the general progression of AI. It may be a very significant step forward, but many companies have been building degrees of AI into their workflow for quite some time. Over half of the organizations in CompTIA's survey (56%) indicate that they have already been working with AI and ML, and generative AI moves that work to another level. Beyond that established group, 36% say that they have not worked with AI/ML before but that they are now seriously exploring generative AI tools, proving the enticing promise of this new technology.

Potential Uses of AI in Cybersecurity



Source: CompTIA 2023 State of Cybersecurity | n=511 U.S. technical and business professionals

As further emphasis of the potential, companies see a wide range of likely uses for AI in cybersecurity over the next two to three years. Many of these behaviors take place today, but they are newer additions to the cybersecurity repertoire (such as analyzing user behavior patterns rather than relying on authorized access to secure perimeters). As businesses face an uphill climb in adding new capabilities without dramatically expanding resources, they will certainly consider AI as a tool that can help handle the growing complexity.

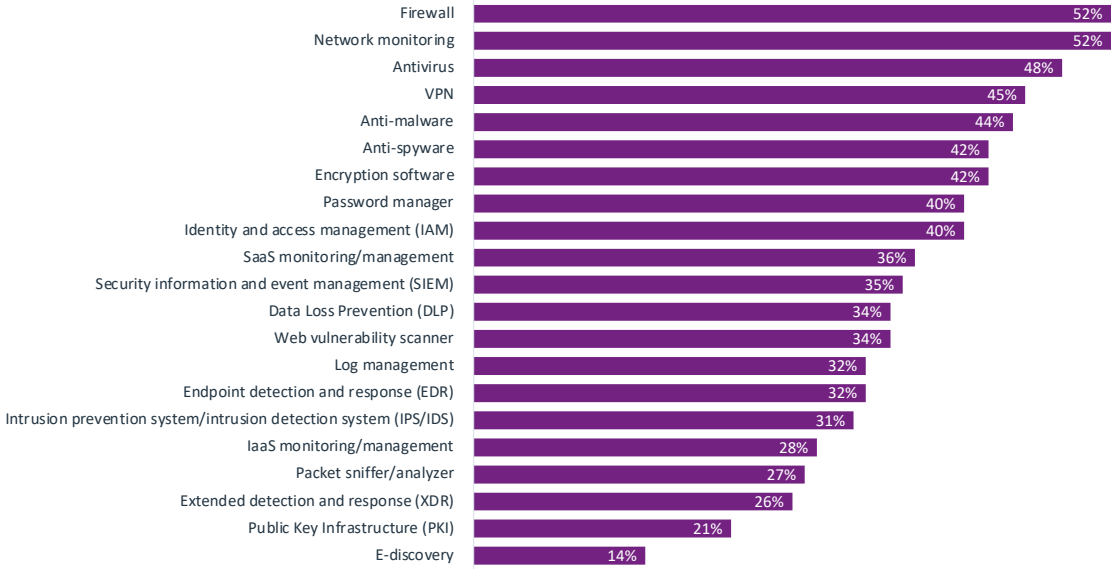
Other potential uses are more novel. Predicting areas where breaches might occur or generating tests for cybersecurity defenses leverages the power of AI to find hidden patterns. In these cases, AI is helping break new ground, offering up solutions that are only achievable through intensive computation of large data sets and complicated mathematical modeling.

As these use cases and many others emerge over the coming years, there several aspects to modern AI that are important to remember. First, AI tools require massive data sets to make inferences. For the most part, the products that have taken the world by storm over the past year are trained on public internet data. Many companies continue to struggle in building their own comprehensive data sets that would be suitable for training, especially the type of training that could produce company-specific insights. Initiatives around data management and analysis are taking on new importance since data is the prerequisite for AI.

Second, AI produces probabilistic results. Unlike more traditional software that produces the same deterministic output on a stable set of inputs, AI algorithms calculate on-the-fly results based on inputs and statistical algorithms. Many times, these results bring forward surprising insights that lead to business opportunities. Other times, the results are incorrect or inappropriate.

The final point, then, is that AI is unlikely to be a replacement for human workers in most cases. Since one reliable use of AI is to automate routine tasks, job roles solely consisting of such tasks may be threatened. Most business cases will require employees to work alongside AI by feeding the correct data, monitoring the results and transforming the output into action plans. To the extent that this activity amplifies productivity, AI may actually become a catalyst for expanded hiring of the necessary skills.

Cybersecurity Products in Use



Source: CompTIA 2023 State of Cybersecurity | n=511 U.S. technical and business professionals

Of course, AI is like other emerging technologies: Not a standalone product by itself, but an embedded component of other products. The cybersecurity toolbox has been steadily expanding over the past few years, and now the challenge of managing a wide variety of cybersecurity tools is compounded by weaving AI capability into each one.

AI may be the newest concern in cybersecurity product management, but it is certainly not the only one. It is interesting (and surprising) to note that there are not major gaps in reported tool use between respondents in a business function and respondents in a technology function. On the positive side, this could indicate healthy levels of communication between business and technology departments around cybersecurity tools and architecture. On the negative side, this could indicate guesswork by both groups based on name recognition vs. detailed knowledge of what is actually in place.

There is also little in the way of trending movement comparing year-over-year product adoption numbers. There are two possible explanations here as well. Again, there could be guesswork involved. Outside of dedicated specialists, a general business employee or even a technology employee outside the area of infrastructure is likely unaware of which products are being employed. In addition, growing complexity of the overall IT architecture may make certain product distinctions difficult as security functionality may be baked into tools primarily used for cloud infrastructure management or data analysis.

In the end, the products being used for cybersecurity along with the personnel implementing tactics and the processes supporting policy are all telling the same story. If there is a balancing act between ideal cybersecurity and productive business operations, achieving that balance has become a highly specialized skill. A rapidly broadening technology footprint leads to an increasing number of profitable vulnerabilities for attackers, resulting in an extremely complicated scenario for security professionals. Each part of an organization owns some responsibility for cybersecurity, but only those with the proper training and expertise can bring all the pieces together for a minimal risk solution.

Methodology

This quantitative study consisted of an online survey fielded to business and IT professionals involved in cybersecurity during Q2 2023. A total of 511 professionals based in the United States participated in the survey, yielding an overall margin of sampling error at 95% confidence of +/- 4.4 percentage points. For international regions (ANZ, ASEAN, Benelux, DACH and UK/Ireland), 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.

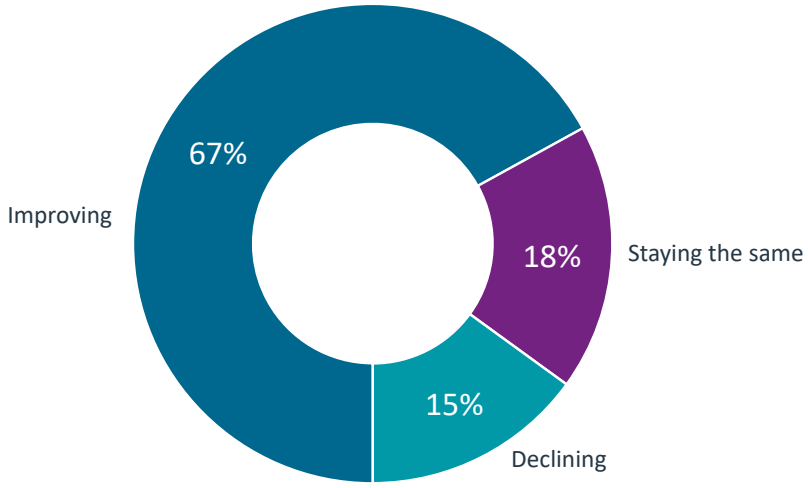
About CompTIA

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.

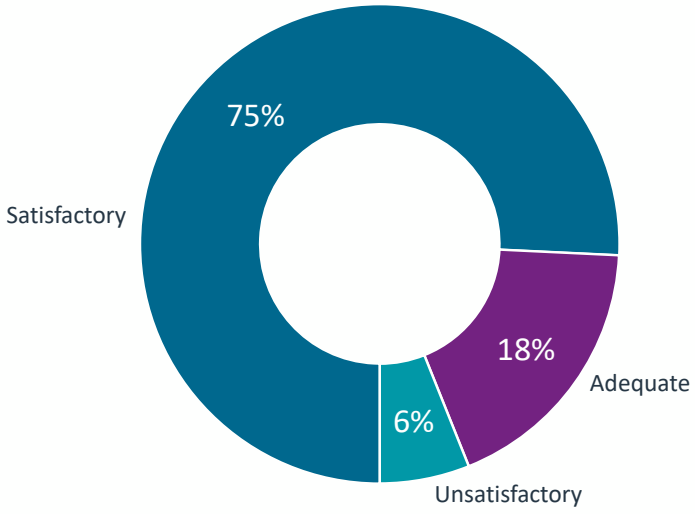
Appendix

Impressions of the Overall State of Cybersecurity



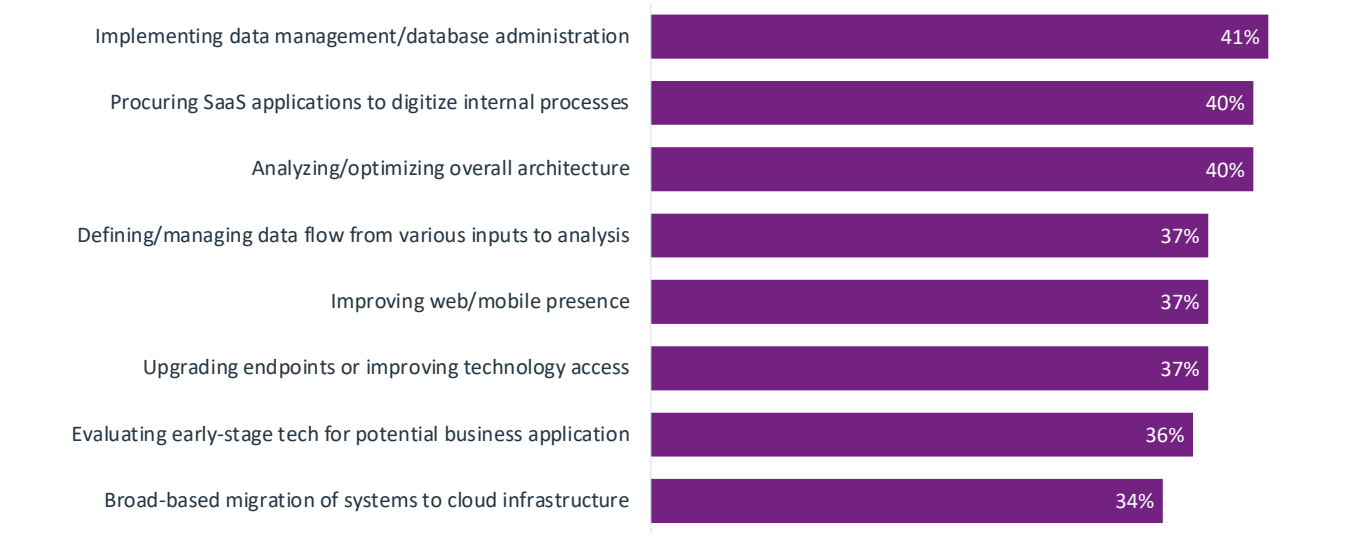
Source: CompTIA 2023 State of Cybersecurity | n=511 U.S. technical and business professionals

Satisfaction with Organizational Cybersecurity



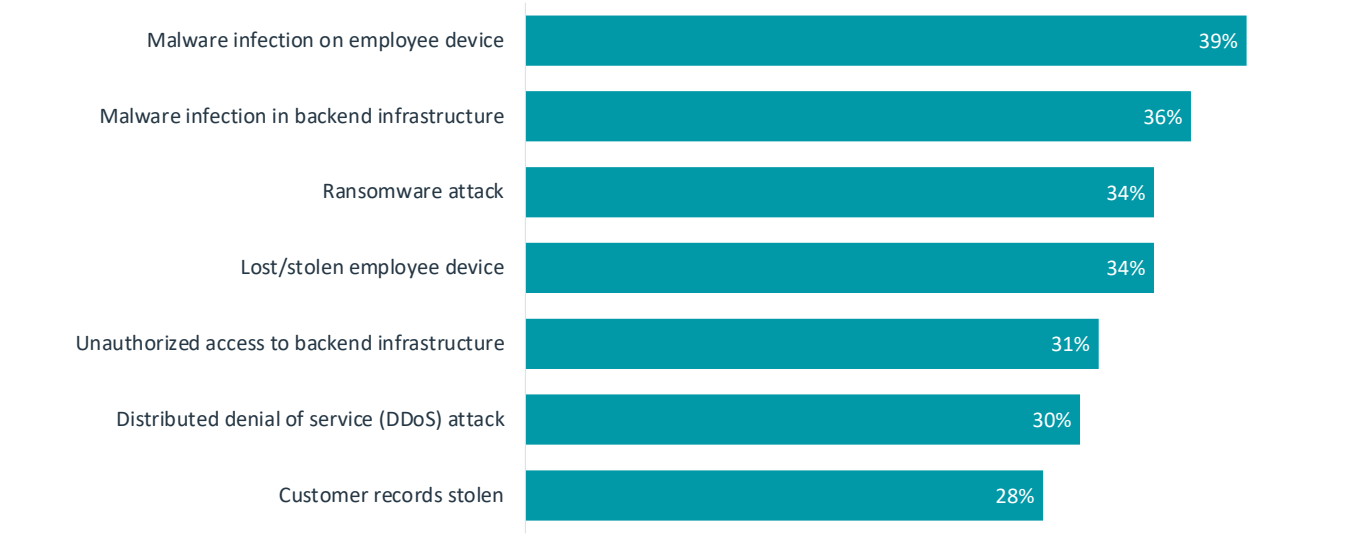
Source: CompTIA 2023 State of Cybersecurity | n=511 U.S. technical and business professionals

Current Technology Initiatives



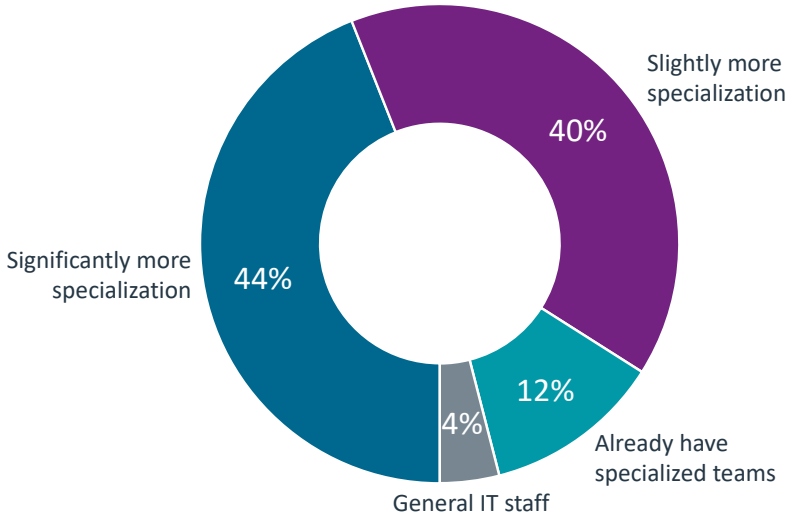
Source: CompTIA 2023 State of Cybersecurity | n=511 U.S. technical and business professionals

Cybersecurity Incidents in the Past Year



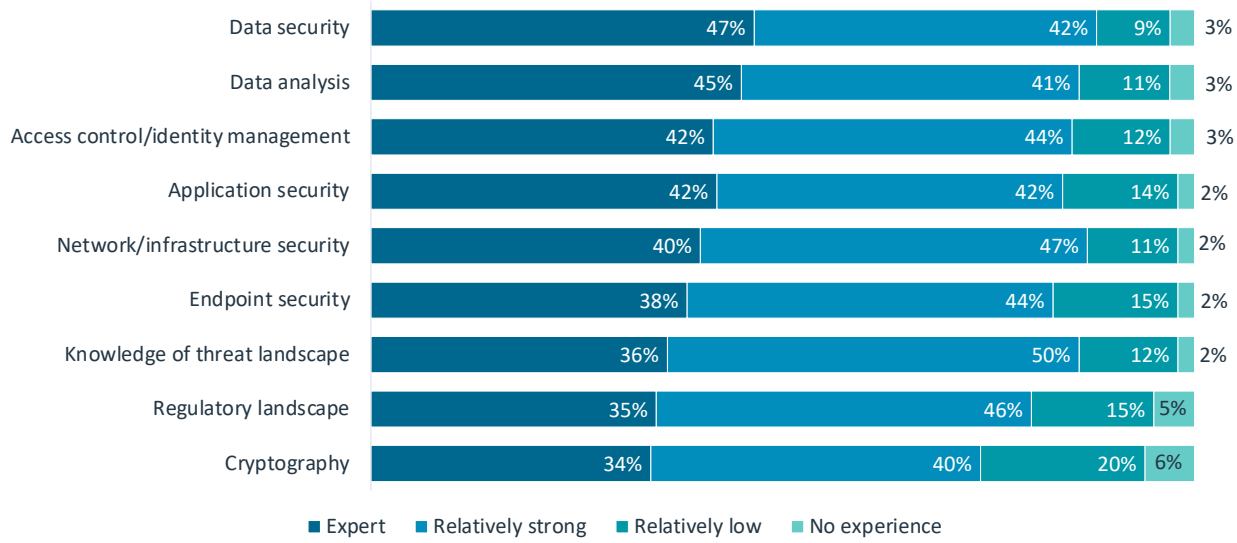
Source: CompTIA 2023 State of Cybersecurity | n=511 U.S. technical and business professionals

Approaches to Cybersecurity Personnel



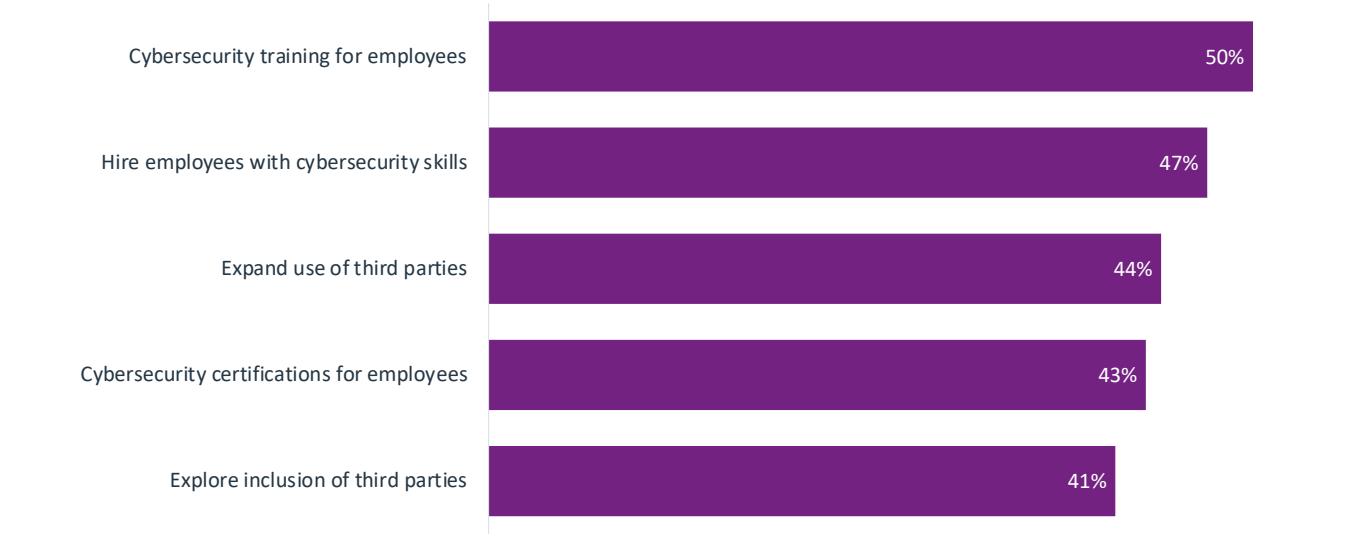
Source: CompTIA 2023 State of Cybersecurity | n=511 U.S. technical and business professionals

Self-Assessment of Cybersecurity Skills



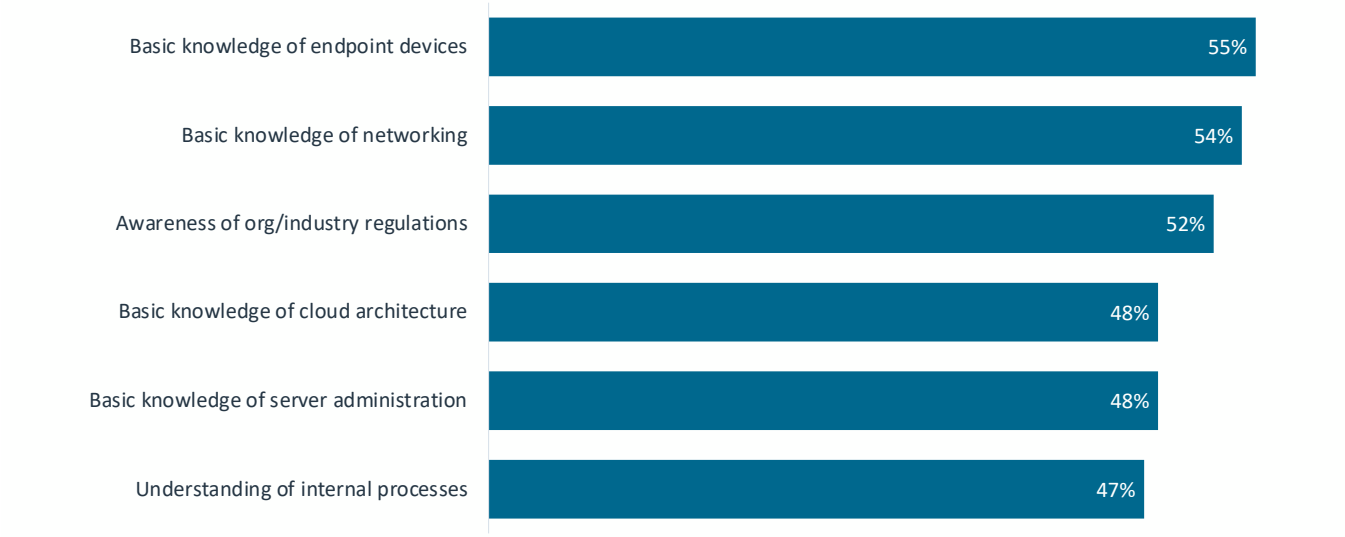
Source: CompTIA 2023 State of Cybersecurity | n=511 U.S. technical and business professionals

Methods of Improving Cybersecurity Skills



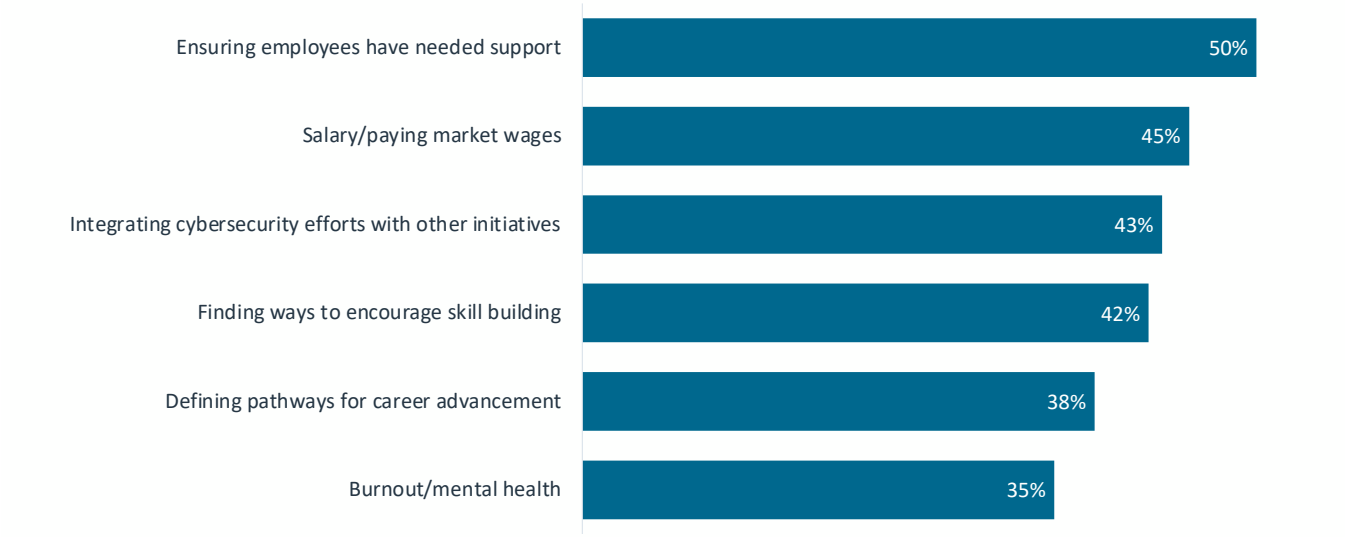
Source: CompTIA 2023 State of Cybersecurity | n=511 U.S. technical and business professionals

Prerequisite Knowledge Needed for Cybersecurity



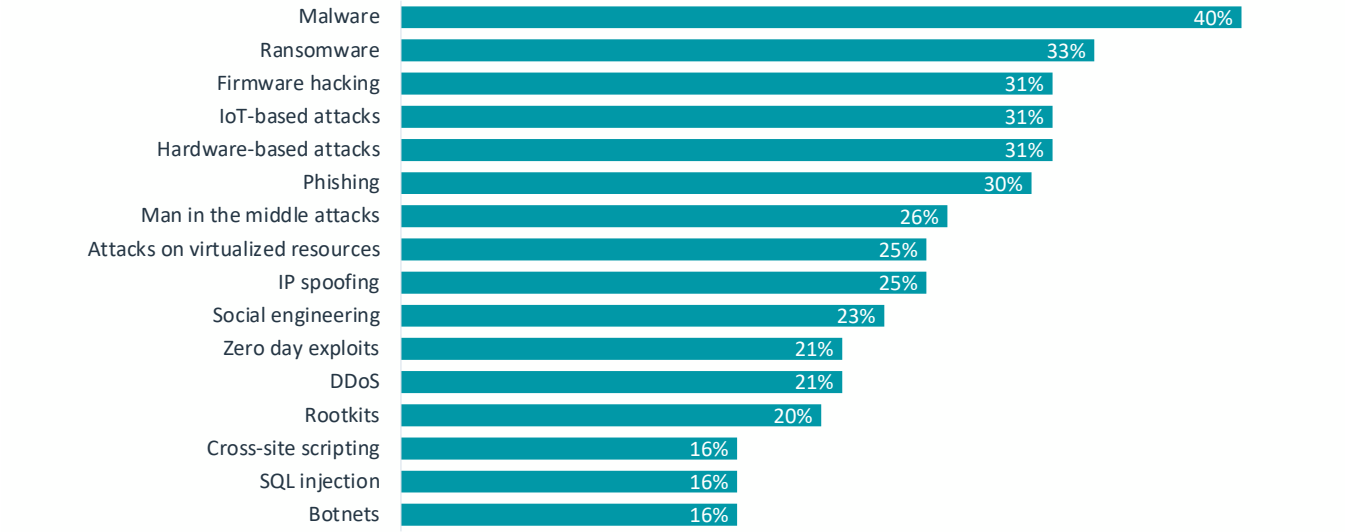
Source: CompTIA 2023 State of Cybersecurity | n=413 U.S. technical and business professionals

Challenges to Retaining Cybersecurity Personnel



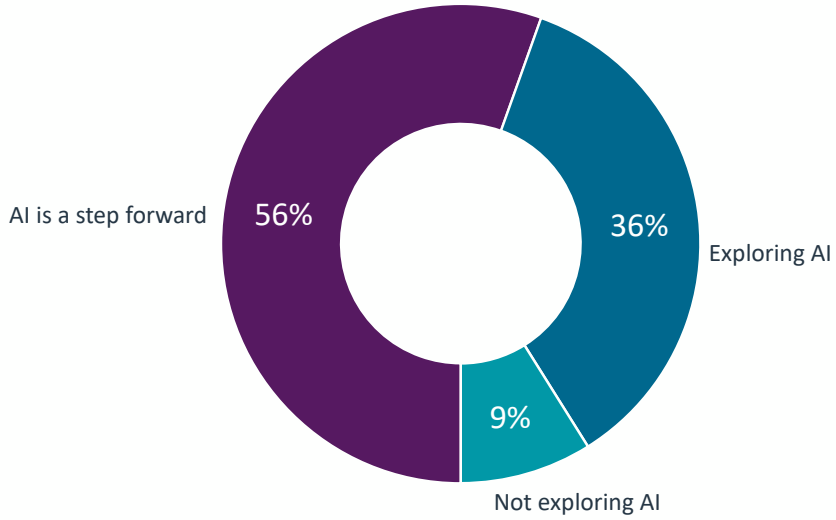
Source: CompTIA 2023 State of Cybersecurity | n=413 U.S. technical and business professionals

Organizational Threat Focus Areas



Source: CompTIA 2023 State of Cybersecurity | n=511 U.S. technical and business professionals

Organizational Approaches to Generative AI



Source: CompTIA 2023 State of Cybersecurity | n=511 U.S. technical and business professionals

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.