CompTIA

State of Cybersecurity 2025

Developing strategy using enterprise architecture

Cybersecurity by the Numbers

$200 billion

IDC projection for global cybersecurity product revenue in 2028

470,000

U.S.-based job openings with cybersecurity-related skills

47%

cite emergence of generative AI as a driver for cybersecurity action

78%

cite cybersecurity as a high priority at their organization

59%

report a severe or moderate impact from cybersecurity incidents in the past year

56%

plan to pursue training for cybersecurity workforce to close skill gaps

Introduction

For most of the 2020s, the technology industry seemed to be an irresistible force. During the pandemic, technology products and occupations were held up as the key drivers enabling pivots to remote work and online commerce. In the recovery phase, organizations doubled down on technology investments and hiring in an effort to quickly regain any lost momentum. Following the immediate recovery, technology continued to offer horizons for future growth, especially with the introduction of generative artificial intelligence (AI).

In mid-2024, the irresistible force met the immovable object of market realities. Tech hiring slowed along with hiring across the general economy as companies grappled with rising interest rates and the complexity of digital transformation. While AI hype remained high, questions of cost and efficacy started popping up, and the CrowdStrike incident in July highlighted the fragile nature of highly integrated technology stacks and the perpetual need for human intervention when technology goes awry.

The slowdown will be temporary, as all market cycles are. The larger question is what lessons businesses will learn from the current conditions. The digital fatigue and frustration that marked the early stages of the correction were a sign that organizations have not fully embraced a mindset and culture around strategic technology and the challenges of building tech-enabled workflows.

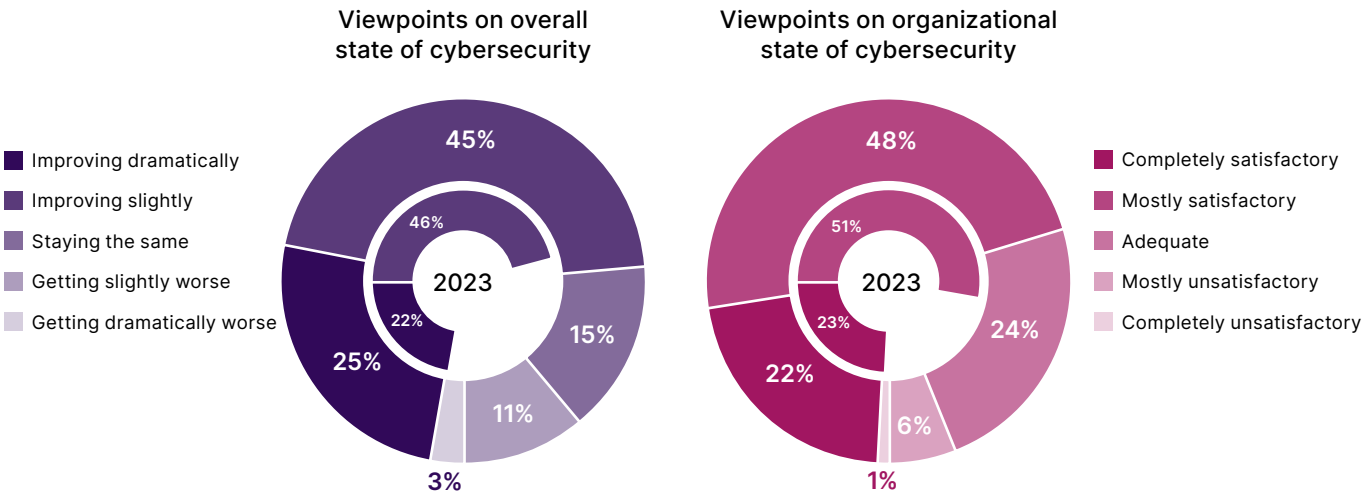
One of the constant themes in CompTIA's State of Cybersecurity reports has been that the field of cybersecurity has changed drastically. Rather than being focused on which technology products can provide the best defense, cybersecurity must now be a proactive process that not only safeguards digital assets but also ensures privacy of data, compliance to regulations and reliability of operations. If there has been slow adoption around a strategic approach to technology, there has also been slow adoption around a modern methodology for cybersecurity.

Traditional market metrics paint a rosy picture for the future of cybersecurity. IDC reports that global revenue for cybersecurity products grew 15.6% between 2022 and 2023 (compared to Gartner's estimated 3.3% growth in overall IT spending). For the five years following 2023, IDC expects the cybersecurity market to continue growing at a double-digit pace, reaching $200 billion in 2028.

From a jobs perspective, CompTIA's Cyberseek tool reports nearly 470,000 U.S.-based job openings with cybersecurity-related skills between May 2023 and April 2024, demonstrating the broad demand for cybersecurity skills across many different job roles. For dedicated cybersecurity roles, CompTIA's State of the Tech Workforce 2024 reports that U.S. cybersecurity employment is projected to grow 267% above the national growth rate.

There remains a disconnect, though, between planned investments and perceived results. Across the six global regions surveyed in CompTIA's State of Cybersecurity 2025 study, only 25% of individuals feel that the overall direction of cybersecurity is improving dramatically, and only 22% would characterize their organization's cybersecurity efforts as completely satisfactory.

Slow progress on positive viewpoints indicates a need for a different approach

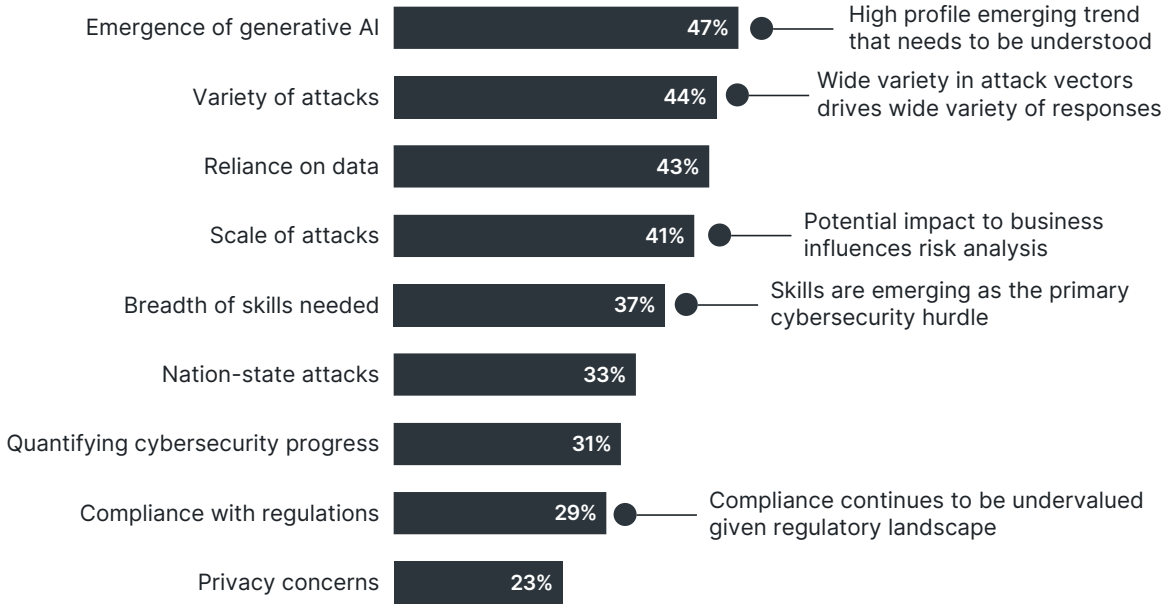


Source: CompTIA State of Cybersecurity 2025 | n=1,181 | 2023 n=1,167

These data points have been stuck in neutral for several years now. While there is substantially more sentiment around slight improvements or mostly satisfactory results, the critical nature of cybersecurity would imply a desire to be at the highest end of the scale. Something is missing, either in the approach organizations are taking or in the expectations around what ideal cybersecurity would look like.

The list of issues currently driving cybersecurity concerns further highlights the challenges companies face in addressing weak points in their adoption strategies. Gone are the days when achieving cybersecurity improvement was a simple matter of purchasing updated technology. Today's cybersecurity issues require businesses to have ongoing discussions around not just the cybersecurity technology stack, but also processes that ensure protection of assets and organizational structure that provides cutting-edge expertise.

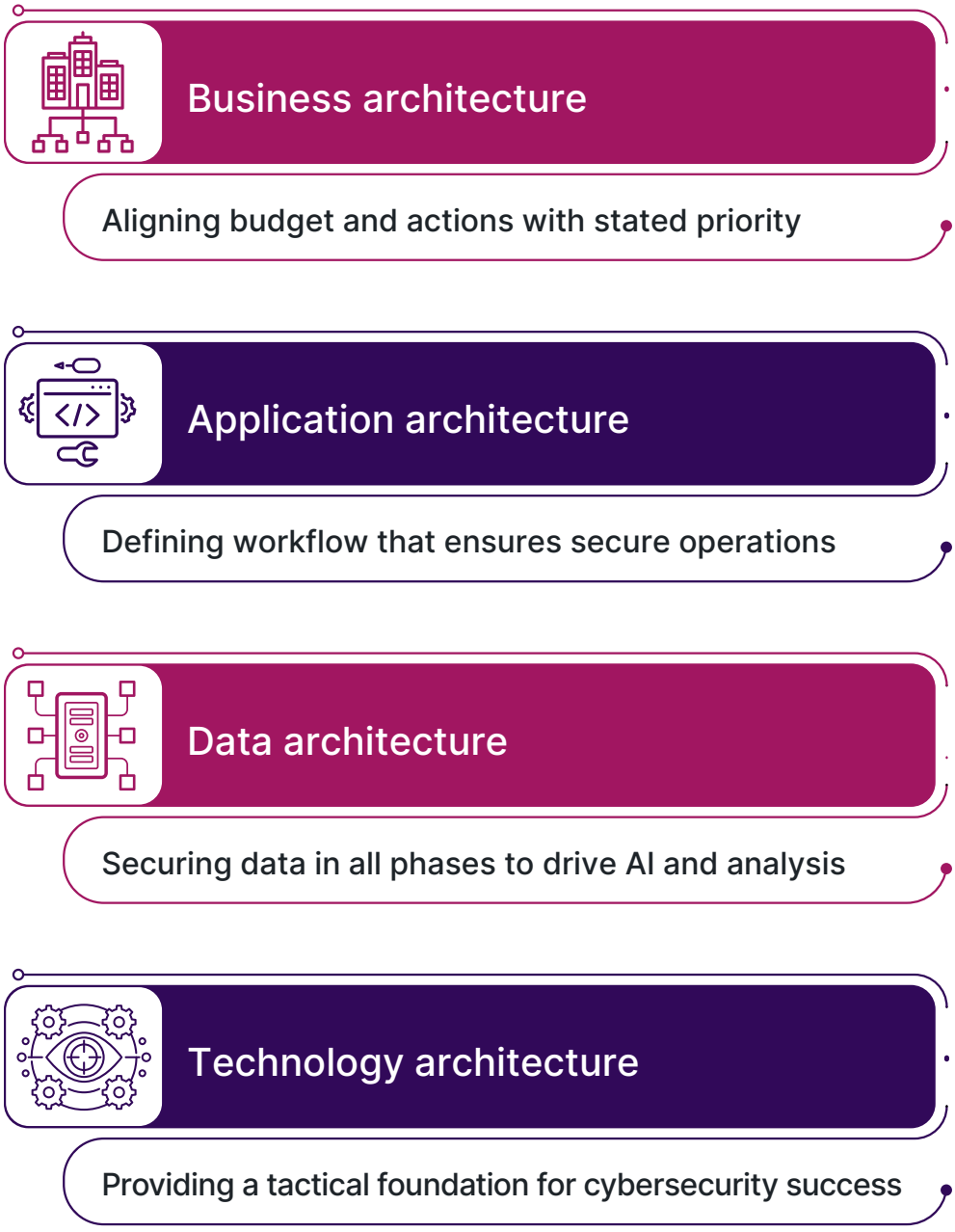
Drivers for cybersecurity point to a wide range of potential actions



Source: CompTIA State of Cybersecurity 2025 | n=1170

The remainder of this report focuses on North American data. Regional breakouts are available in related research briefs.

Cybersecurity imperatives across the enterprise architecture framework

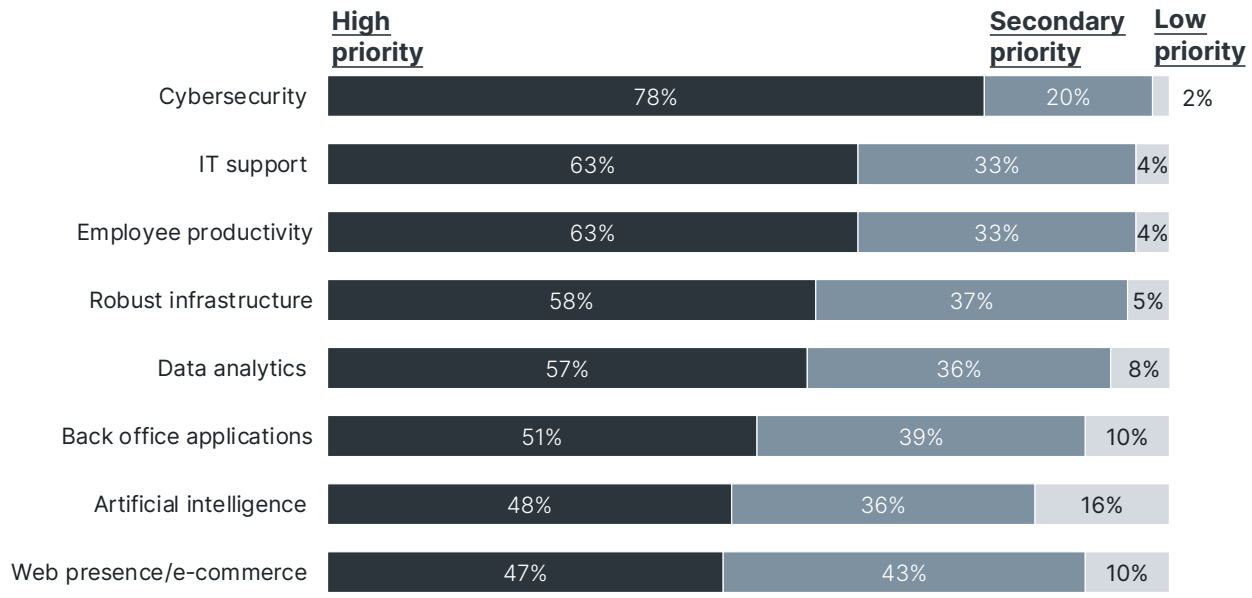


The dilemmas of a strategic technology mindset and a robust cybersecurity approach are tightly intertwined. Cybersecurity efforts must not only respond to changes in technology operations, but also influence the decision process more heavily than in the past. As organizations solve both sides of the equation, the four layers of the enterprise architecture model can provide a structure for making decisions. Starting with a broad business perspective and drilling down through applications, data and technology will help set priorities and identify tradeoffs as companies move toward effective cybersecurity.

1 Business Architecture

For the most part, applying the enterprise architecture model to overall technology efforts will call attention to issues across all four primary technology domains (infrastructure, software, data and cybersecurity). However, cybersecurity is unique among these domains in that it has a more direct impact on business viability. As such, cybersecurity has become a business imperative with considerations for all levels of an organization—staff, management, executives and governing bodies. This significance allows the enterprise architecture model to be applied directly to cybersecurity efforts alongside broader technology strategy.

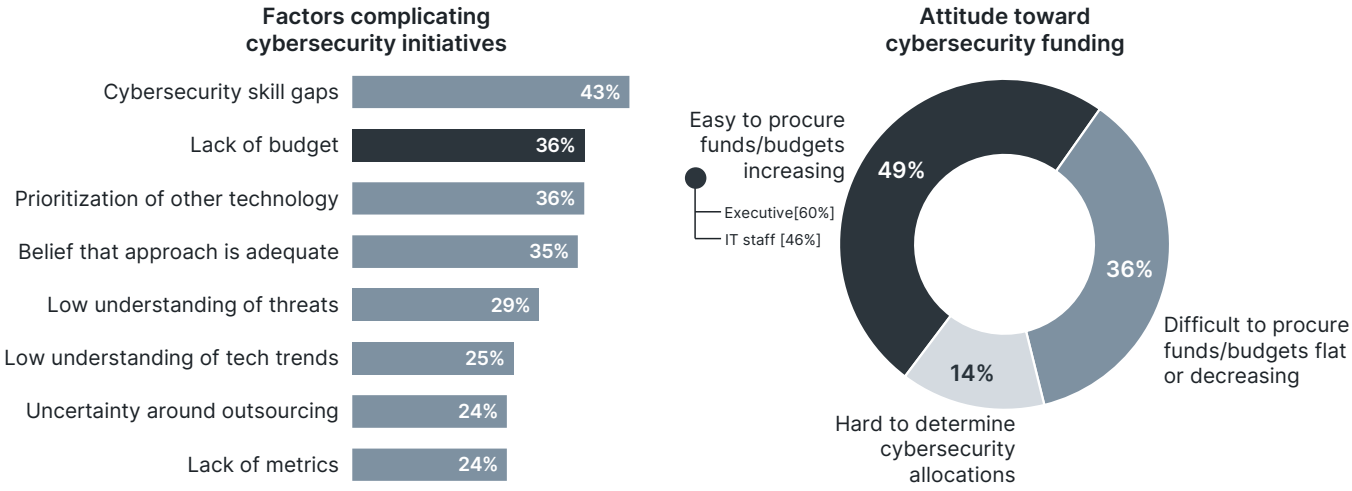
Cybersecurity takes the top spot for perceived organizational priority



Source: CompTIA State of Cybersecurity 2025 | n=525

At the business architecture level, the main issue to resolve is the ongoing operational process around cybersecurity based on the priority within the organization. The first question, then, is what priority the firm places on cybersecurity. While the data may be somewhat skewed in coming from a cybersecurity-focused survey, it is no surprise to see that cybersecurity ranks as the top priority among many different technology initiatives, at least in terms of perception. Cybersecurity incidents are high-profile with broad impacts, so it makes sense that organizations would assign a high priority.

Budget issues show that cybersecurity remains difficult for organizations to resolve



Source: CompTIA State of Cybersecurity 2025 | n=525

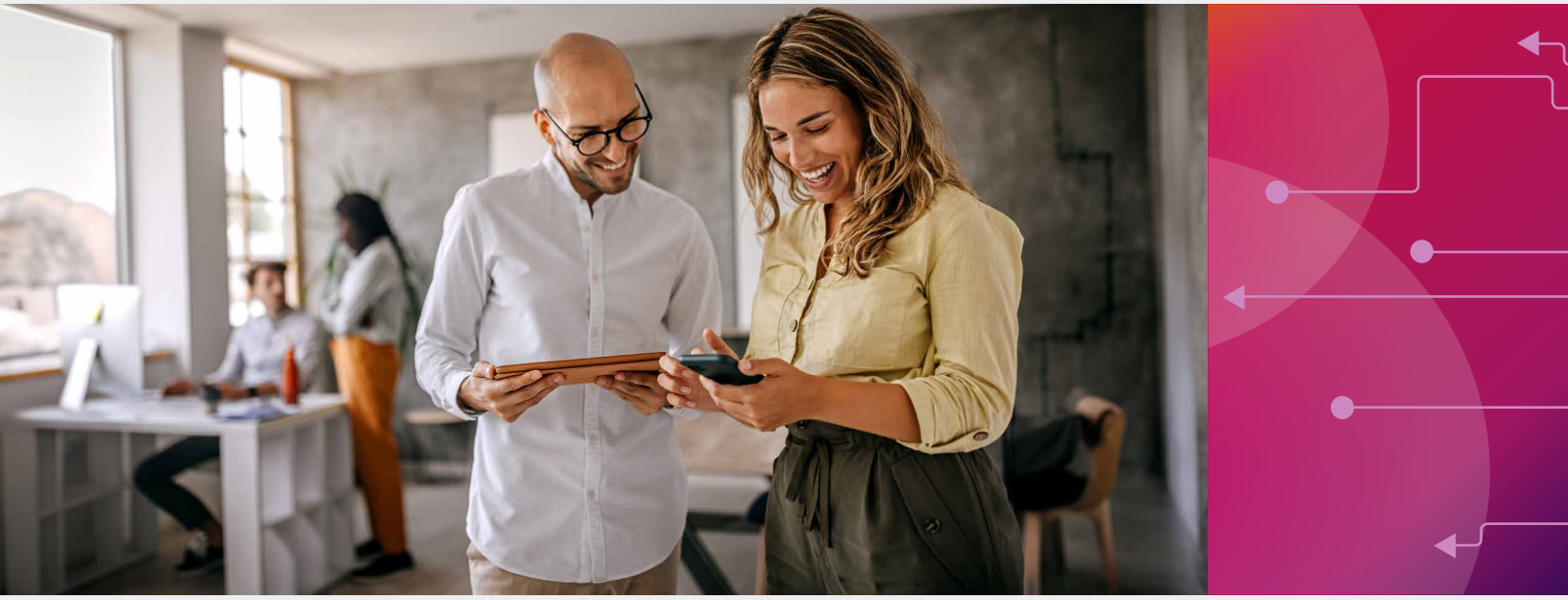
However, aligning internal behavior with stated priority is where the disconnects start to become apparent. The first place this surfaces is in budget allocations. For several years, CompTIA's study found that the main difficulty in pursuing cybersecurity initiatives was in overcoming institutional mindset around the need for improved measures. Last year, skill gaps took the top spot as a primary hurdle. This year, lack of dedicated budget and emphasis on other technology initiatives joined the skills issue as major challenges.

Carving out cybersecurity budget numbers is notoriously difficult because of the way cybersecurity is woven into other activities. Choosing a cloud infrastructure provider or performing a compliance audit may be driven by other departments, but the cybersecurity team clearly plays a large role. With that said, the general attitudes around cybersecurity funding point to a discrepancy between stated priority and available budget. While 78% of respondents state that cybersecurity is a high priority at their firm, only 49% feel that it is relatively easy to procure funds for cybersecurity activities or feel that cybersecurity budgets are increasing. Even that number around funds may be elevated, as 60% of executives say that cybersecurity funding is relatively easy to procure compared to only 46% of IT staff.

Establishing agreement on processes aligned with priority requires collaborative effort. For business leaders, this may involve an examination of corporate structure, whether that means the composition of the cybersecurity team or the involvement of cybersecurity within governing practices. For cybersecurity leaders, this will require a deeper understanding of how cybersecurity impacts business viability. The proficiency in describing these high-level effects comes from incorporating cybersecurity principles at lower layers of the enterprise architecture model.

The Two Sides of Governance

In cybersecurity discussions, “governance” typically brings to mind issues around regulatory compliance. This is especially true in highly-regulated industries, such as healthcare or finance, or in different geographic regions. While the need for compliance is real and growing, there is a broader view of governance that businesses should consider. The fields of cybersecurity and data are not quite as well-established as the fields of infrastructure and software development, where decades of experience have led to documented frameworks and best practices. In cybersecurity, best practices have emerged around specific topics, such as risk analysis or incident response, and these individual pieces are beginning to coalesce into a holistic framework, but that framework still needs to be integrated more into corporate strategy. For cybersecurity professionals, properly balancing both aspects of governance will be critical in defining long-term plans.



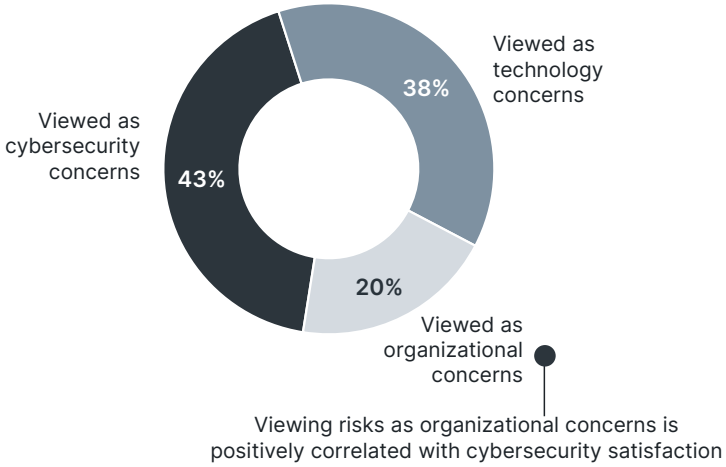
2 Application Architecture

There are differing viewpoints on the ordering of the next two layers in the model. From one perspective, the data layer is more foundational than the individual applications used for internal operations. On the other hand, the applications combine into an overall workflow, and defining this workflow drives implications for technology decisions. This report will adopt the more comprehensive view of application architecture.

Risk analysis is a critical component of defining workflow, and it has also become the guiding principle for cybersecurity efforts. The exact practices of risk analysis are somewhat objective from one organization to another, but CompTIA's data shows relatively strong adoption of formal or informal risk analysis procedures. As expected, use of a formal framework such as the NIST Risk Management Framework or the IRGC Risk Governance Framework is more prevalent among larger companies. That is offset somewhat by a larger percentage of small and medium-sized businesses who perform informal risk analysis, making risk management a familiar concept for most.

Risk analysis and mitigation should be an organization-wide process

Viewpoints on risks identified through analysis



Top elements involved in risk analysis

53% Use of cloud computing

47% Technology procurement

44% Data classification

42% Mobile devices

Source: CompTIA State of Cybersecurity 2025 | n=511

Once again, though, the details matter. Most importantly, the output of risk analysis is often not considered as a broad organizational concern. The vast majority of businesses view risk analysis as an activity confined within the technology function, with more than four in ten firms further stating that risk analysis is specific to the cybersecurity specialists.

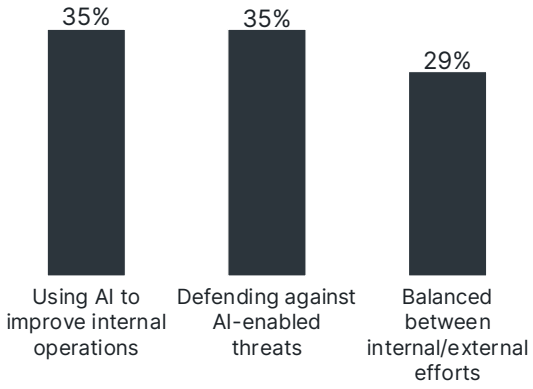
To be sure, the risks most commonly identified in analysis center around technology elements. The core components of cloud usage, tech procurement, data classification or mobile device implementation are all tech-related; however, the analysis should not be limited to the specific security measures for each of these components. The costs and tradeoffs of security choices should be evaluated in the context of organizational goals.

Today, the most prominent technology component featuring in both corporate aspirations and cybersecurity analysis is artificial intelligence. Although AI has been a part of emerging technology discussions for several years, the arrival of generative AI kicked off a new hype cycle. Naturally, businesses are eager to capture whatever value they can from this new trend. The ability to do so will depend on a solid understanding of how AI fits into an evolving technology stack.

As with any hype cycle, initial excitement is beginning to run up against implementation obstacles. Across a standard four-stage adoption curve, 41% of firms identify as performing education/pilot programs and 36% identify as performing low-priority implementations. This places the majority of businesses at the beginning of an AI journey, which is typical for new technology but perhaps contrary to expectations created by media and cutting-edge enterprise firms. History tells us that progress will be impeded by factors both internal and external, with slow additions to the 16% of firms citing high-priority implementations and the 7% of firms citing full transformation of workflows.

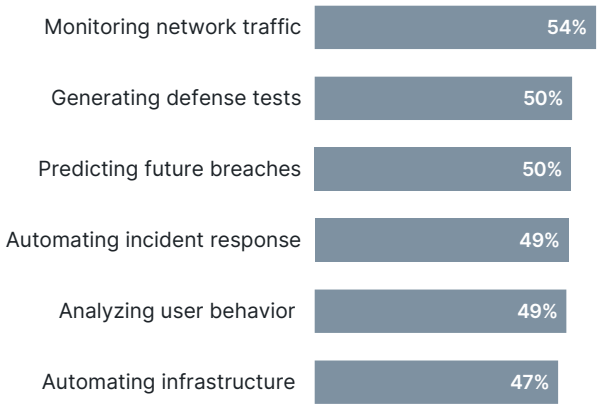
AI has potential to automate and accelerate cybersecurity efforts

Priority for AI within cybersecurity



Balanced viewpoints reflect shift in cybersecurity objectives from defensive measures to proactive initiatives

AI-enabled cybersecurity use cases



Source: CompTIA State of Cybersecurity 2025 | n=525

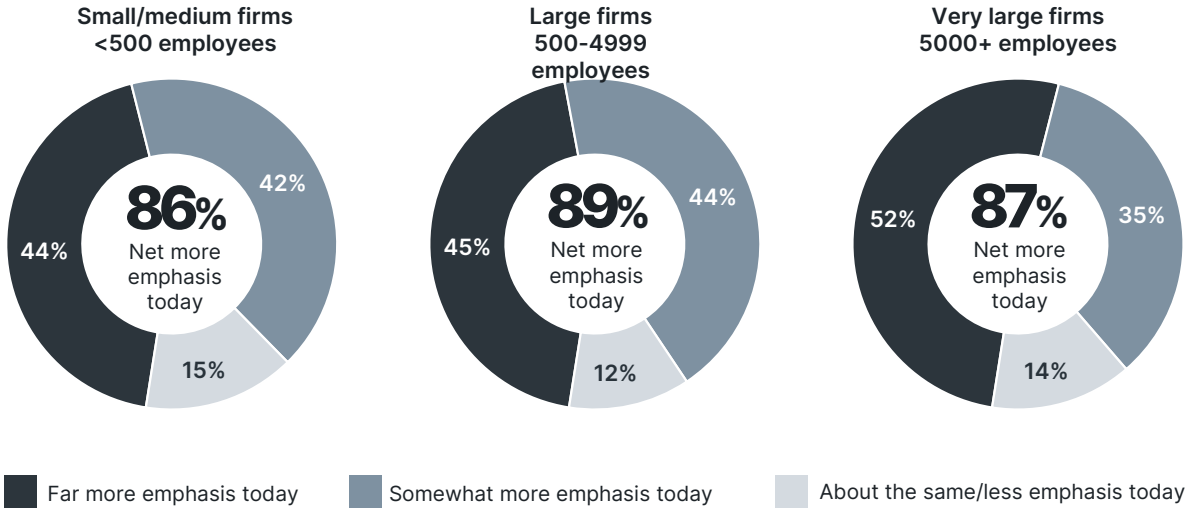
From a cybersecurity perspective, AI plays on both sides of the action. Companies are evenly split between an emphasis on using AI internally to improve their defense and an emphasis on learning about new forms of AI-enabled attacks. Either approach demonstrates the way that AI simply adds to the complexity of modern cybersecurity. The expected use cases involve a range of activities where businesses already face struggles, such as automation and data analysis.

3 Data Architecture

Data architecture follows application architecture from a decision-making perspective, but clearly not from a priority perspective. Overall, 46% of firms say they place far more emphasis on data today compared to two years ago. Very large companies lead this charge, powered by the resources they can apply toward data management and analysis. Executives also drive this sentiment, as data analytics and visualization have led to greater data-driven decision making.

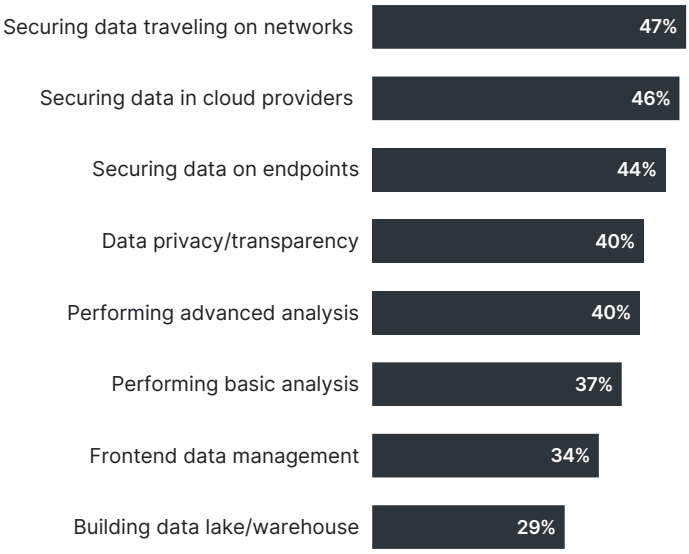
There are several reasons for data's rise in importance, and there is significant overlap between the fields of data and cybersecurity. As computing resources became somewhat commoditized across companies (especially with the adoption of cloud computing), data became a critical area to build differentiation. More recently, the strong interest in AI has accelerated the need for robust practices that produce data fit for training AI algorithms.

Data is a far greater point of emphasis today compared to two years ago



Source: CompTIA State of Cybersecurity 2025 | n=525 | Smaller n for subsegments

High focus areas in the field of data have strong correlation with cybersecurity



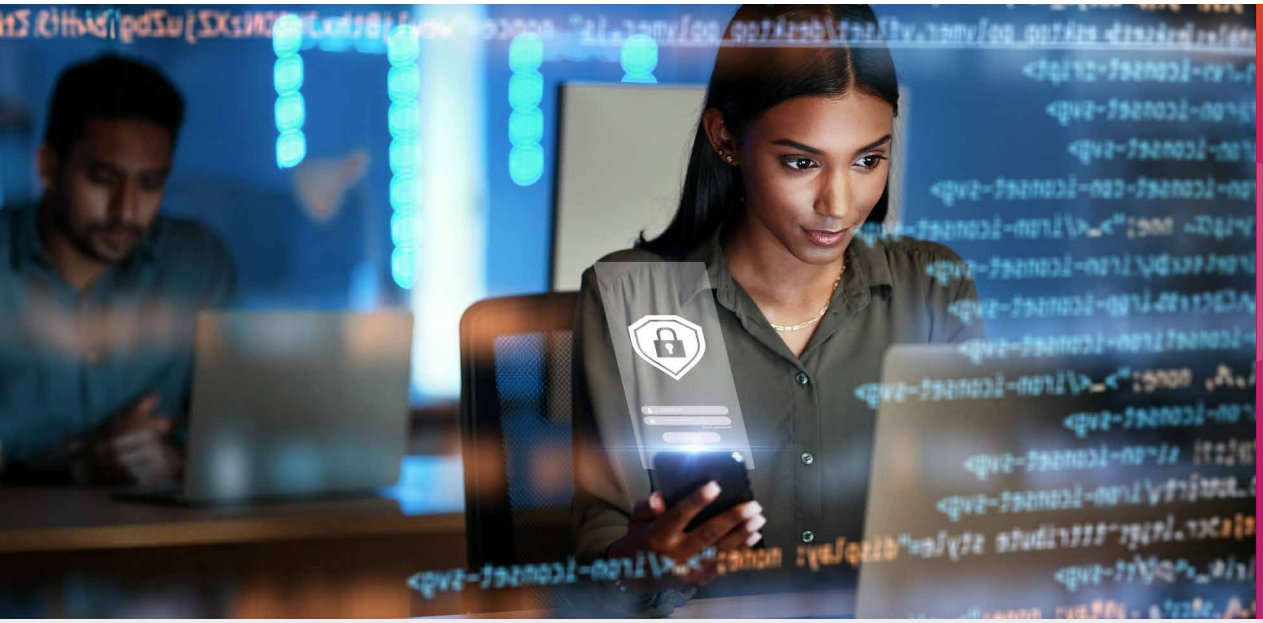
Along with securing data at rest, in motion and in use, organizations are engaged in building foundational data management practices that enable advanced techniques. The rise of AI has accelerated the need for robust data practices in order to properly train AI algorithms, and the demand for data science continues to be strong as businesses seek competitive differentiation.

Source: CompTIA State of Cybersecurity 2025 | n=525

This dependence on data leads to the first overlap with cybersecurity. Among many different elements of data management and analytics, securing data is clearly top of mind. The elimination of secure perimeters for cloud operations led to focused security for both data and applications, and cybersecurity teams are still building methodologies to protect data in each phase of use. Securing data is perhaps the leading tenet of a zero trust framework, as corrupt data that is unverified can have a devastating impact on data-dependent operations.

A second overlap between data and cybersecurity takes place as cybersecurity experts perform their own data analysis while monitoring threats and responding to incidents. The combination of digital acceleration and resource constraints creates an overwhelming amount of information for cybersecurity professionals to digest, so advanced data analysis techniques along with automation are critical for staying on top of things.

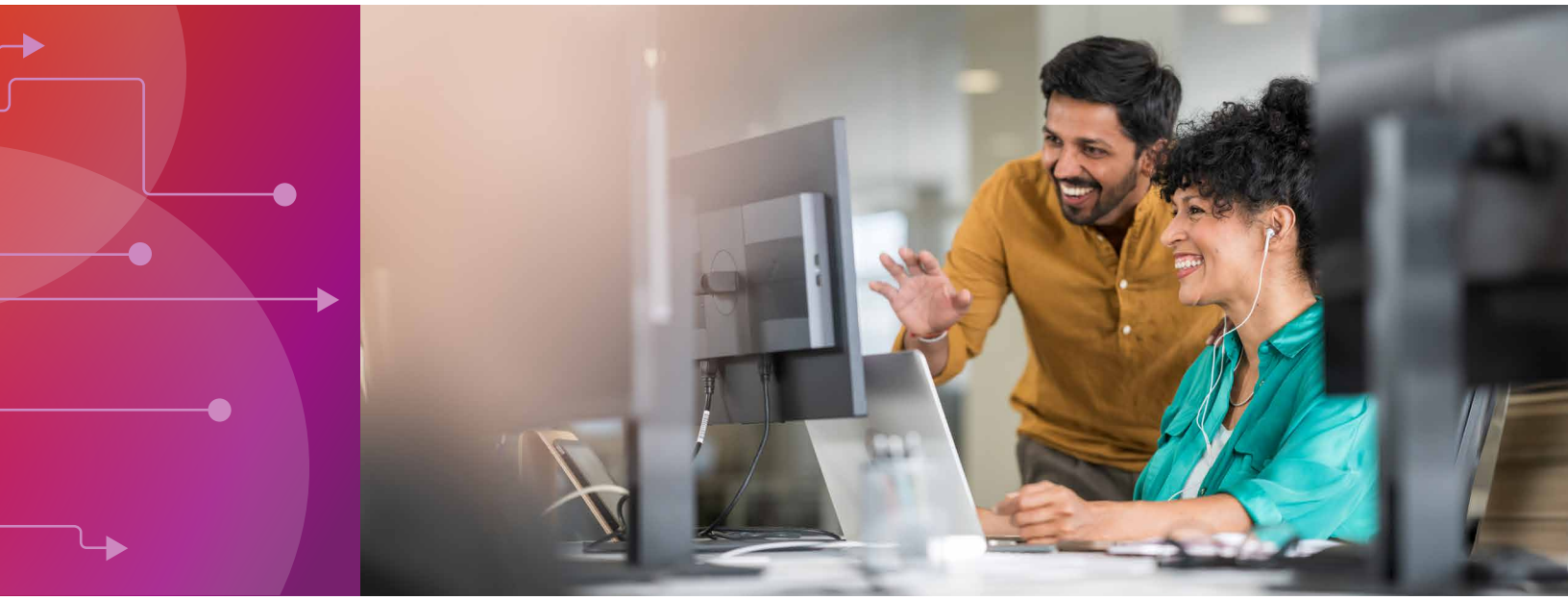
Finally, data can help undergird new metrics that organizations are using to define success or progress with cybersecurity strategy. While only 29% of companies say that they have started using new cybersecurity metrics in the past year, 38% of executives identify new metrics as a key process change. This indicates the need to incorporate cybersecurity as part of the discussion around business health, and this need will only grow as companies drive their objectives with technology.



The Value of Zero Trust

Over the past five years, "zero trust" has become the leading candidate for the new mindset around cybersecurity. If the old mindset could be defined as "secure perimeter," zero trust provides guidance around how to think about data, applications and user behavior in a modern digital environment. As with so many labels, though, the term can be confusing. Given the product-centric history of cybersecurity and the current collaborative efforts between cybersecurity teams and business leaders, there can be questions around which products or initiatives are classified as zero trust. The lack of metrics to prove zero trust success further complicates the picture. Since many specific actions contribute to a zero trust framework, cybersecurity professionals should focus on these elements (such as identity and access management or multi-factor authentication) rather than emphasizing zero trust with executive stakeholders. This will provide more discrete definitions for investment and success, and zero trust can remain a guiding light used internally by cybersecurity teams.

4 Technology Architecture



At the lowest layer of the enterprise architecture model, the focus turns to tactics. Here is where the situation most closely resembles a traditional view of cybersecurity, with technology products integrated into a comprehensive solution that protects against attacks and mitigates risk.

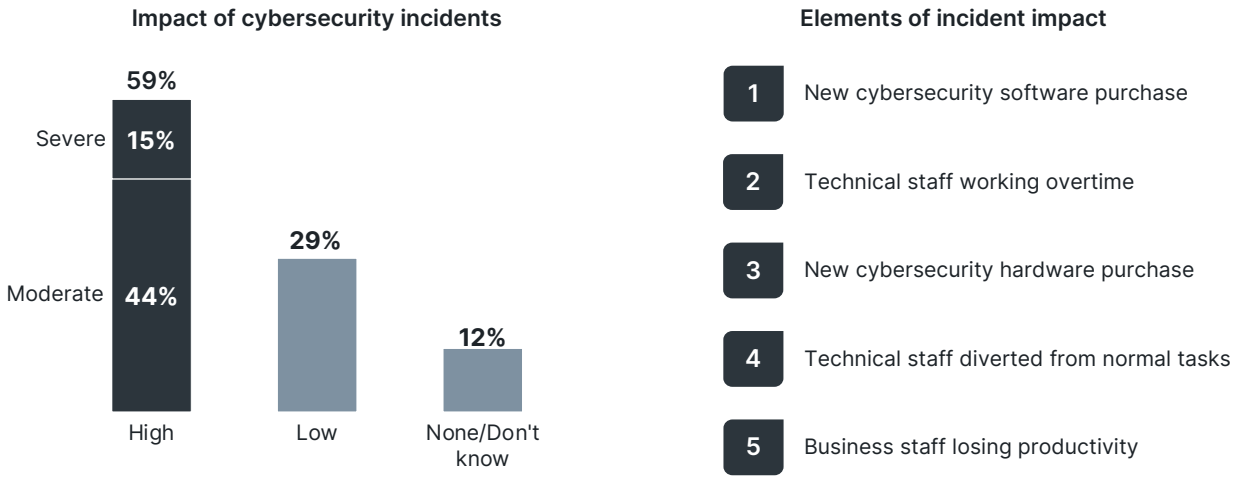
The dynamic threat landscape presents the first tactical challenge for cybersecurity professionals. To start, there are longstanding threats that still run rampant as bad actors target organizations with weak cybersecurity. Malware has certainly evolved over the decades, but many core principals remain the same—as do the common defenses. Even so, malware is listed as a top three concern that organizations want to understand better.

The other two concerns in the top three are ransomware and phishing, attack vectors that have emerged more recently and have proven extremely potent for cybercriminals. One interesting note about these two threats is that technology plays less of a role in prevention and mitigation. Instead, well-defined processes and effective end user training are key elements in avoiding damage.

These three threats alone require significant time and effort in monitoring and mitigation, but there are a wide range of other threats that must be taken into account. Supply chain attacks take advantage of automated software update processes and complex technology stacks. Data poisoning complicates a data management process that many companies are in the early stages of building. Cyber extortion is a variant of ransomware where the attackers threaten to make data public rather than simply making it unusable.

Of course, outside forces are not the only—or the largest—concern for organizations. Internal human error continues to play a significant role in cybersecurity event. Phishing and social engineering rely on end users making mistakes, and these attacks have become incredibly sophisticated. In addition, the most common cybersecurity incident cited by companies is the old standby of a lost device.

Cybersecurity incidents cause high amounts of disruption

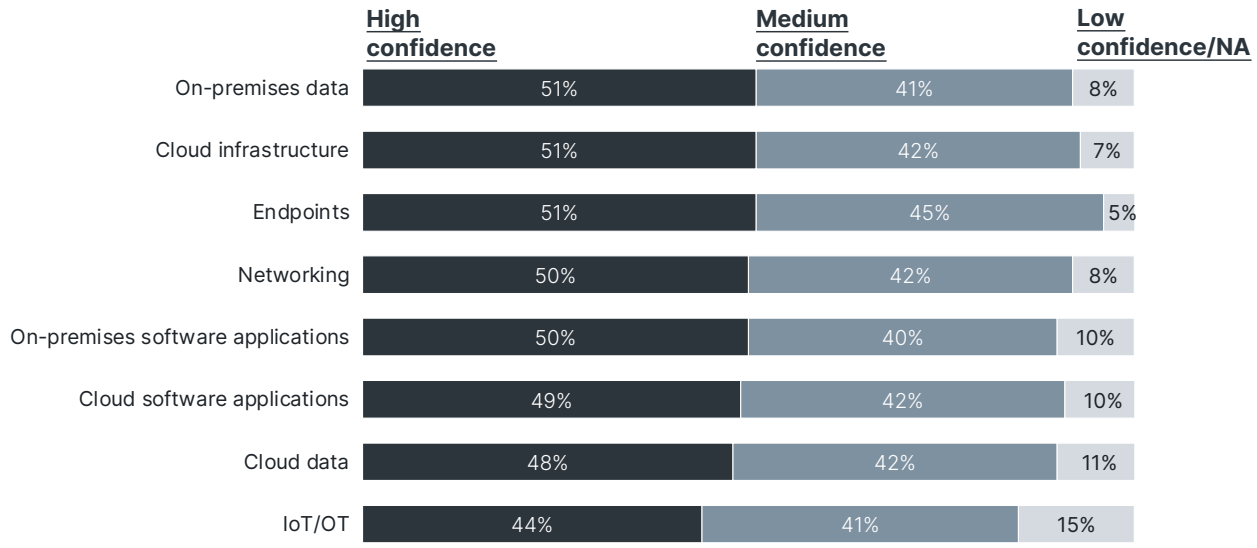


Source: CompTIA State of Cybersecurity 2025 | n=525

When it comes to the impact of cybersecurity incidents, the data shows why cybersecurity remains a hot button for most firms. Nearly six in ten businesses say that the impact of cybersecurity incidents in the past year has been moderate to severe, with clear downsides for both finances and productivity. It is an oversimplification to say that cybersecurity remains a priority because the problem has not been solved, but the fact remains that cybersecurity is a discipline that many organizations still struggle to fully understand.

That struggle largely stems from the explosion in complexity that cybersecurity teams are asked to address. Sixty percent of firms say that they have over 1,000 assets under management, including endpoints, cloud systems and operational technology (OT). OT in particular provides a good example of the complex environment, as cybersecurity professionals have to understand physical infrastructure components such as building utility systems or manufacturing equipment that has been digitized and network-connected.

Confidence is questionable for cybersecurity coverage across all asset classes



Source: CompTIA State of Cybersecurity 2025 | n=525

The sobering reality is that there is relatively low confidence in the level of visibility and control across all asset categories. IT staff, who might be expected to have the best knowledge of cybersecurity capabilities, consistently rate as the group with the lowest levels of confidence. When cybersecurity dealt with a lower number of threats targeting a smaller attack surface, the job could be handled as a portion of overall infrastructure responsibilities. Today's environment demands a different approach and much deeper skills.

5 Building Cybersecurity Skills

Just as organizations must consider multiple layers in their cybersecurity strategy, there is a growing need to build multiple layers of cybersecurity expertise. The practice of relegating cybersecurity responsibilities to technology generalists is quickly fading. Professionals in every tech discipline must have some degree of cybersecurity acumen related to their field, and there are many highly specialized roles being explored within dedicated cybersecurity teams.

Businesses continue to show a predilection toward internal resources as the foundation of cybersecurity efforts. Over half of all firms state that they utilize either in-house dedicated cybersecurity professionals or other in-house technology professionals as part of their staffing strategy. Compared to 2023, there was a slight increase in the number of firms with dedicated staff.

Third-party resources remain an important part of the resource equation for many firms, with approximately one-third of companies utilizing either specialized cybersecurity providers or partners that provide a variety of technology services. Larger firms are more likely than their smaller counterparts to use specialized providers or consultants, pointing to an opportunity for technology firms servicing small clients to add more cybersecurity-focused offerings to their portfolio.

Data around skill level and improvement need suggests lack of detailed skill awareness

	Skill level				Need to improve		
Skill domain	**Expert**	**Relatively strong**	**Relatively low**	**No experience**	**Significant need**	**Moderate need**	**Don't know**
Network/infrastructure security	43%	44%	11%	2%	34%	59%	7%
Knowledge of threat landscape	37%	48%	12%	3%	37%	58%	5%
Application security	39%	53%	8%	1%	35%	58%	7%
Data security	45%	46%	7%	2%	37%	58%	5%
Endpoint security	39%	48%	11%	1%	34%	59%	7%
Identity management	40%	48%	11%	2%	35%	59%	7%
Data analysis	44%	44%	12%	1%	36%	58%	6%
Regulatory landscape	33%	50%	16%	2%	33%	58%	9%
Automation/AI	29%	43%	23%	5%	49%	43%	8%

Source: CompTIA State of Cybersecurity 2025 | n=525

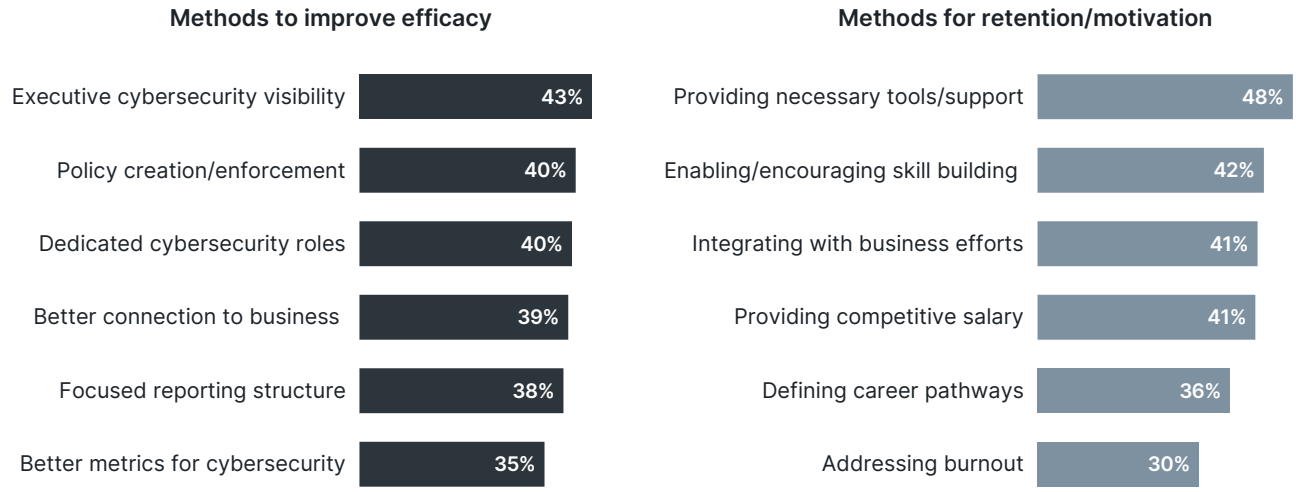
Across both internal and external resources, organizations are building hierarchies of cybersecurity skills. As cybersecurity emerged as a standalone discipline, the first step for many businesses was to develop cybersecurity specialists from an established base of infrastructure professionals. Now that cybersecurity practices are more mature and growing in scope, forward-thinking companies are creating dedicated teams with depth and robust career pathways.

The assessment of and demand for cybersecurity skills provides the impetus for this team-building approach. Consistent with previous CompTIA research, organizations cite significant need for improvement even in areas where they also cite relative strength of skill. Network security is certainly not a new topic, but companies need a cadre of employees focused on the evolutions within this foundational area as they develop targeted skills related to identity management or penetration testing.

A hierarchical approach to cybersecurity skills speaks to the demand for training and certification. Even early-career positions in cybersecurity require some knowledge of technology systems and cybersecurity methodology. Candidates for these positions may demonstrate their knowledge through a variety of educational tracks and achievements; from that point, organizations need to continue providing skill-building options for career development and corporate health.

There is still strong intent to hire for cybersecurity, with 53% of companies considering new hiring as an option. However, intent to hire can be derailed by external forces and prove challenging in even the best cases as businesses fight over a limited pool of expertise. An even greater number of firms (56%) plan to pursue training for their cybersecurity workforce, and 42% plan to offer cybersecurity certifications as a way of establishing core concepts within the team and extending skillsets into emerging focus areas.

Focused efforts are required to maximize efficiency and ensure long-term success



Source: CompTIA State of Cybersecurity 2025 | n=429

Developing skills is the most significant action companies may take in improving efficiency, but there are other options as well. Increasing visibility and awareness among senior executives points all the way back to the beginning of the architectural approach. Establishing organizational imperatives and metrics gives cybersecurity teams a greater stake in future accomplishments. From there, building policies that drive employee behavior will create a culture of cybersecurity that helps the team do their job without additional tension.

Finally, companies need to focus on the long-term outlook for cybersecurity professionals. As with most technology roles, churn and burnout can make it difficult to realize a strategic vision. Along with skill building, the ease of procuring necessary tools and a tight integration with business initiatives can provide the necessary support for engagement and career growth.

As digital efforts push new boundaries, it may be tempting to reduce cybersecurity initiatives back to a simplified view, where a baseline set of technology products provides a relatively reliable defense. This viewpoint would underestimate the complexity of technology integration and the criticality of digital operations. Instead, companies should embrace the challenges of structuring cybersecurity as a business imperative and building the skills necessary for corporate wellbeing and success.

Methodology

This quantitative study consisted of an online survey fielded to business and IT professionals involved in cybersecurity during Q3 2024. A total of 525 professionals based in North America participated in the survey, yielding an overall margin of sampling error at 95% confidence of +/- 4.4 percentage points. This survey was also fielded in ANZ, ASEAN, Benelux, DACH and UK/Ireland. 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.

International region	Sample size
ANZ	134
ASEAN	134
Benelux	128
DACH	128
UK/Ireland	132

About CompTIA

The Computing Technology Industry Association (CompTIA) is the world's leading information technology (IT) certification and training body. CompTIA is a mission-driven organization committed to unlocking the potential of every student, career changer or professional seeking to begin or advance in a technology career. To learn more about CompTIA:

CompTIA Learning and Training

CompTIA Solutions Catalog

CompTIA Career Explorer

CompTIA Job Posting Optimizer

CompTIA IT Salary Calculator

Appendix A

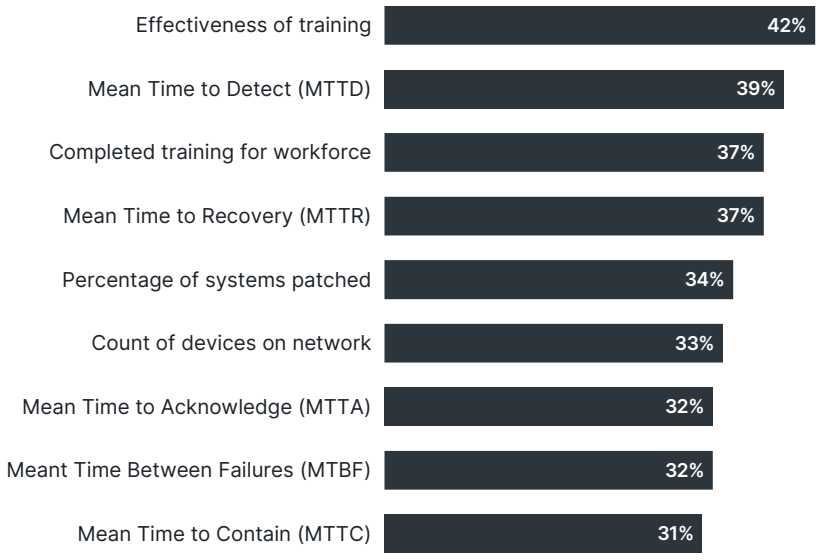
Drivers for cybersecurity point to a wide range of potential actions

	Small	Medium	Large	Very large
More focus on process improvement	33%	32%	46%	38%
More focus on employee education	38%	42%	37%	38%
Greater investment in tech products	47%	45%	47%	45%
User of new metrics	27%	29%	27%	33%
More focus on risk management	36%	33%	38%	47%
Higher priority on incident response	37%	36%	48%	52%
Creation of dedicated resources	17%	27%	32%	38%
Exploration of cyber insurance	24%	29%	28%	24%
Greater use of third parties	31%	34%	33%	35%
Higher awareness of compliance	29%	40%	40%	48%

- Large firms have grown to a point where process is critical
- Very large firms recognize the impact of risks
- Larger firms have more to lose from incidents
- Small firms are resource-constrained and need help with specialization
- Small firms underestimate the role of compliance

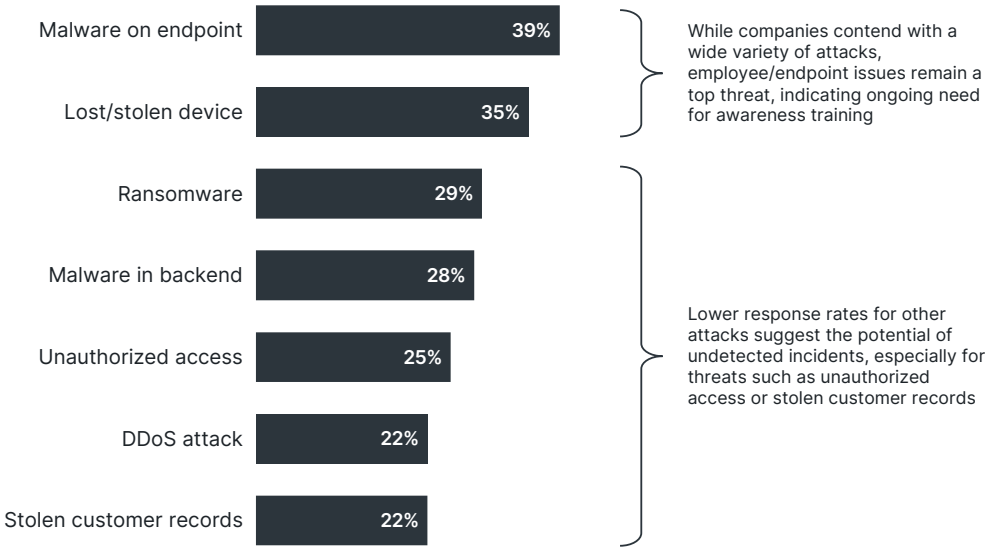
Source: CompTIA State of Cybersecurity 2025 | n=525 | Smaller n for subsegments

Cybersecurity metrics in use cover a range of process components



Source: CompTIA State of Cybersecurity 2025 | n=525

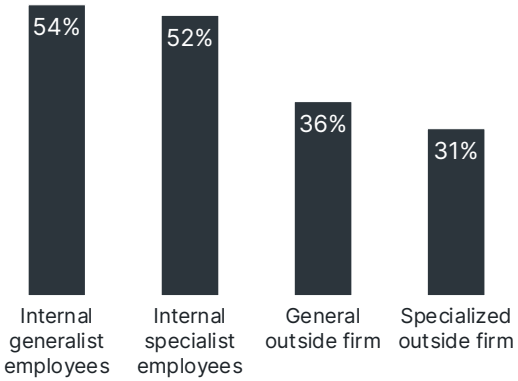
Cybersecurity incidents reflect the challenges in building and executing strategy



Source: CompTIA State of Cybersecurity 2025 | n=525

Organizations mainly leverage internal resources, but third parties play a strong role

Resource groups involved with cybersecurity initiatives



Important criteria when selecting third party

Source: CompTIA State of Cybersecurity 2025 | n=525

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.