CompTIA

State of Cybersecurity 2025

Cybersecurity by the Numbers

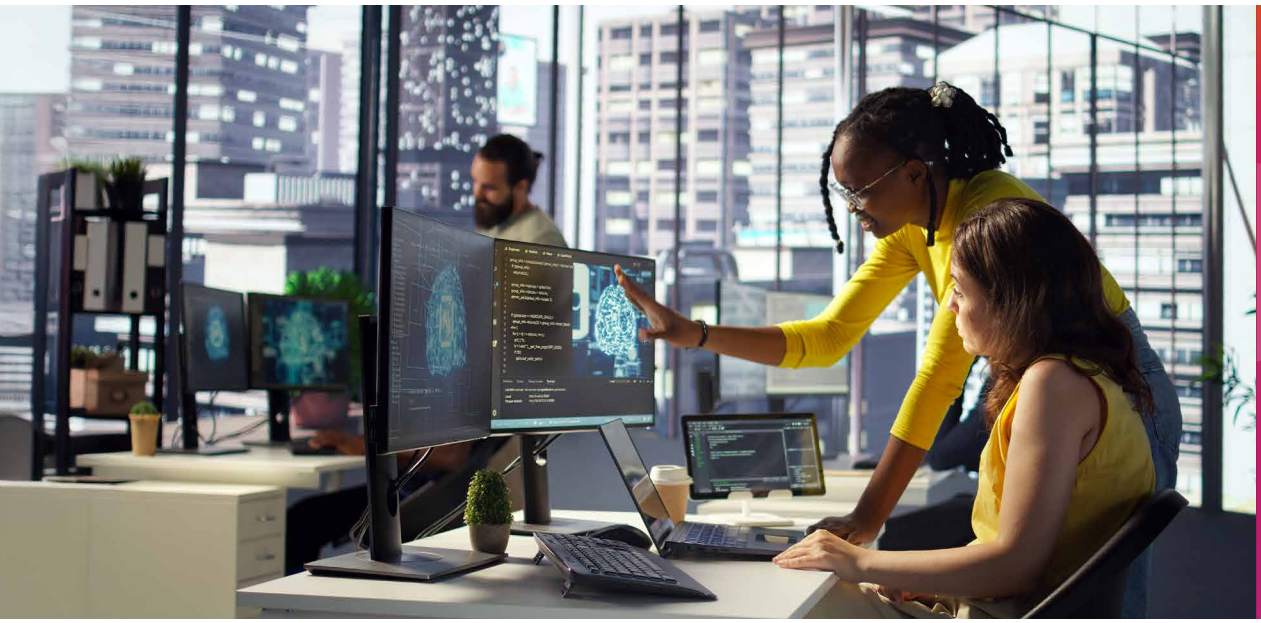
514,000
U.S.-based job openings with cybersecurity-related skills

#1
Rank of skill gaps as a hurdle for cybersecurity strategy

70%
Companies in early stages of AI adoption

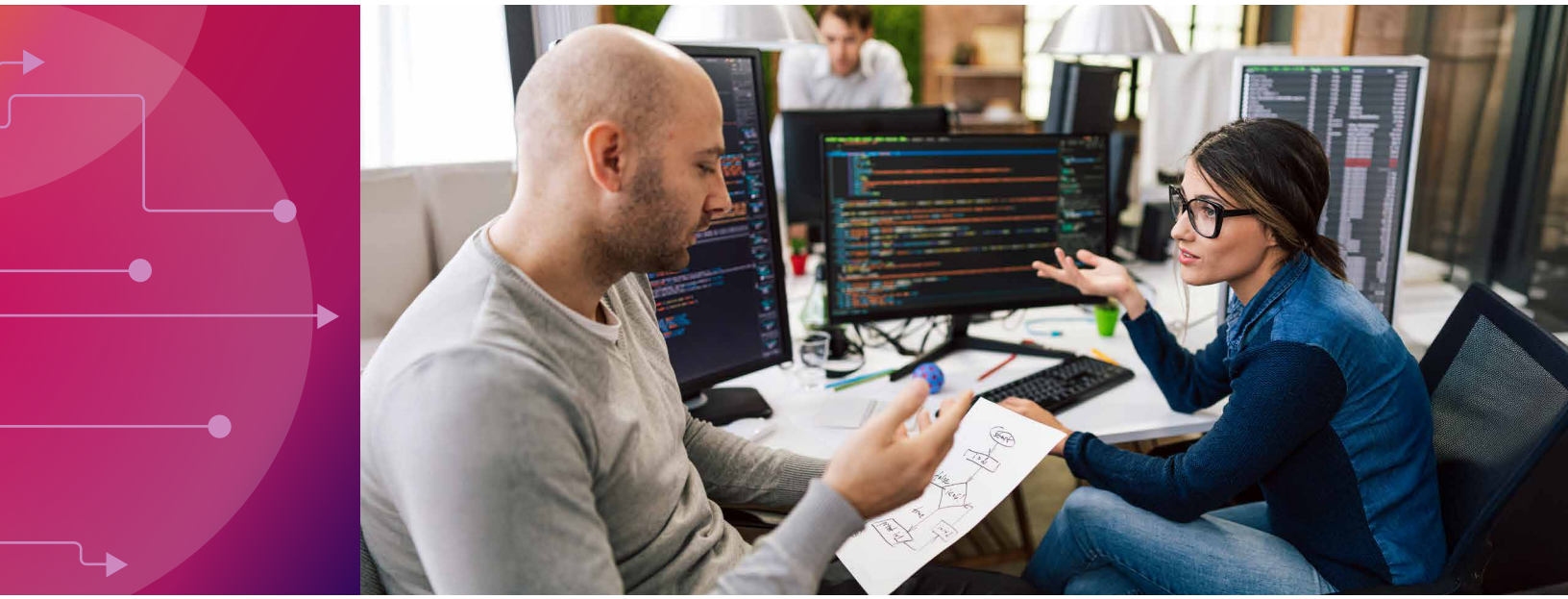
94%
Companies with high/moderate focus on operational technology

73%
Companies rating impact of cyebrsecurity incidents as severe/moderate



Introduction

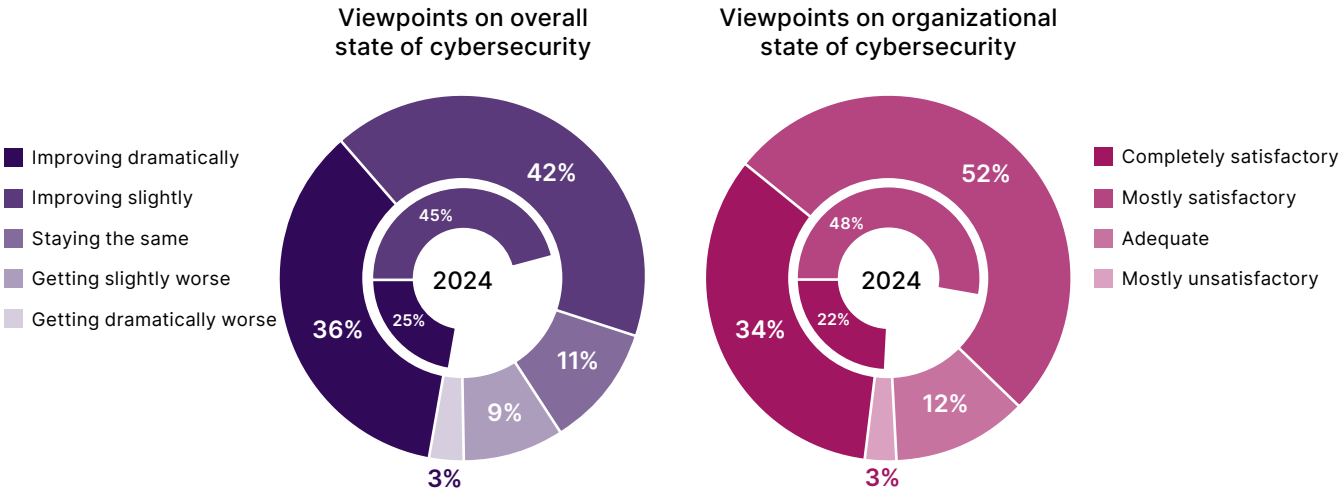
How important is cybersecurity? It may seem like a rhetorical question, but the answer runs surprisingly deep. Unpacking the different layers behind this question requires sifting through perspectives from several different cohorts, from dedicated cybersecurity professionals to business executives, from small businesses to multinational enterprises. There are many different opinions based on many different objectives, and putting all the pieces together helps build a picture of sentiment and best practices across the broader economy.



At the highest level, cybersecurity is a business imperative, as CompTIA's research has previously established. No longer a secondary component of IT operations, cybersecurity has become a discipline that merges technical expertise, regulatory compliance, and corporate behaviors in order to safeguard an organization's assets and operations. Given the reliance on digital workflow in modern business environments, cybersecurity takes on the same level of importance as finance or legal in terms of maintaining organizational health and success.

Just because something is critical, though, does not mean the focus, staffing, or budget should constantly grow. The dynamic nature of cybersecurity can lead to a constant stream of suggestions around what businesses should be doing to counter every threat on the landscape. This information onslaught can lead to fatigue among both business leaders and IT staff as they try to determine how to stay on top of everything. At the same time, improved risk analysis has helped reconcile the nebulous specter of cyberattacks with the real constraints of each organization, allowing companies to become more comfortable with how they apply resources to the most relevant threats.

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

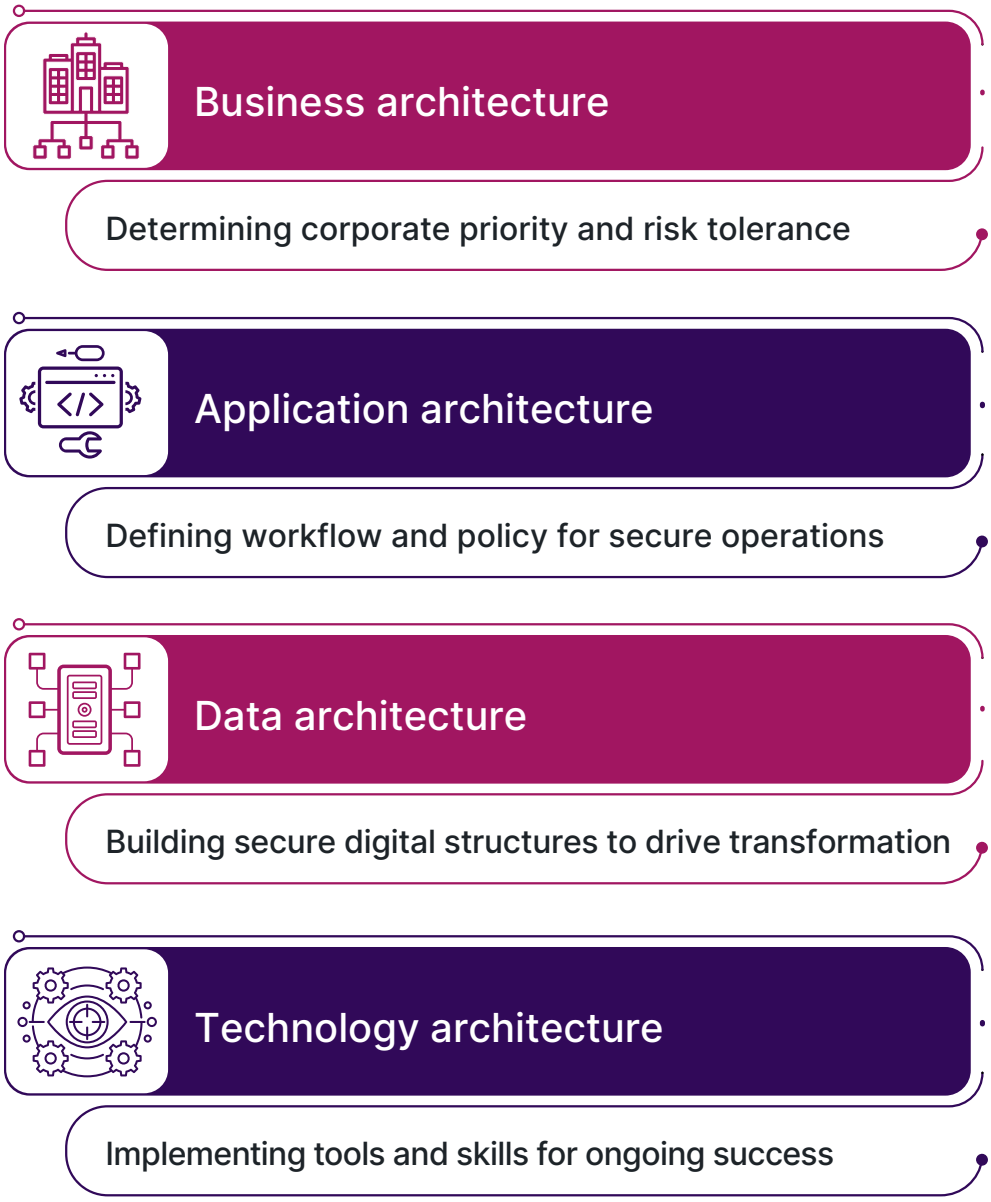


Source: CompTIA State of Cybersecurity 2025 | n=1,026
CompTIA State of Cybersecurity 2024 n=1,181

Whatever the reason may be, there is notable improvement in both sentiment around the general state of cybersecurity and satisfaction with organizational posture. After several years of stationary viewpoints in these two areas, CompTIA's 2025 data shows positive movement. While cybersecurity still ranks at the top of the priority list among technology initiatives (81% rating cybersecurity as a high priority), it also ranks at the top of the list when it comes to organizational capability (68% rating their organization as highly capable). There is still a gap between priority and capability, but companies are pursuing greater balance between dedicated cybersecurity activities and comprehensive technology strategies.

One way of finding this balance is to continue applying the same architectural approach to cybersecurity that gets applied to broader technology systems. The top-down approach of the enterprise architecture framework is a valuable tool in setting corporate culture and policy around cybersecurity before getting into tactical details of implementation and skills. It also provides a feedback loop to help ensure that cybersecurity tactics are instrumental in meeting organizational objectives.

Cybersecurity imperatives across the enterprise architecture framework



Maybe the question of cybersecurity's importance is less about its priority and more about ensuring operational excellence. Although companies seem to be feeling more comfortable with their approaches, the threat landscape continues to shift. McKinsey reports a 1200% increase in phishing attacks since the rise of generative AI in late 2022. Covewear, a division of the cybersecurity software firm Veeam, found that the average ransomware payout in Q2 2025 doubled from only one quarter before. The Ponemon Institute estimates the average annual cost of insider threats at $17.4M. For new approaches to be fully effective, they must be flexible enough to defend against ongoing attacks while appropriately navigating the demands of the business.

1 Drivers, Decisions, and Difficulties

The starting point for building cybersecurity strategy is understanding what forces are shaping risk and response. With cybersecurity expanding beyond a pure technical activity, there are many factors that influence a company's risk assessment, policies, and skill development.

Drivers for cybersecurity underline the importance of a well-rounded approach

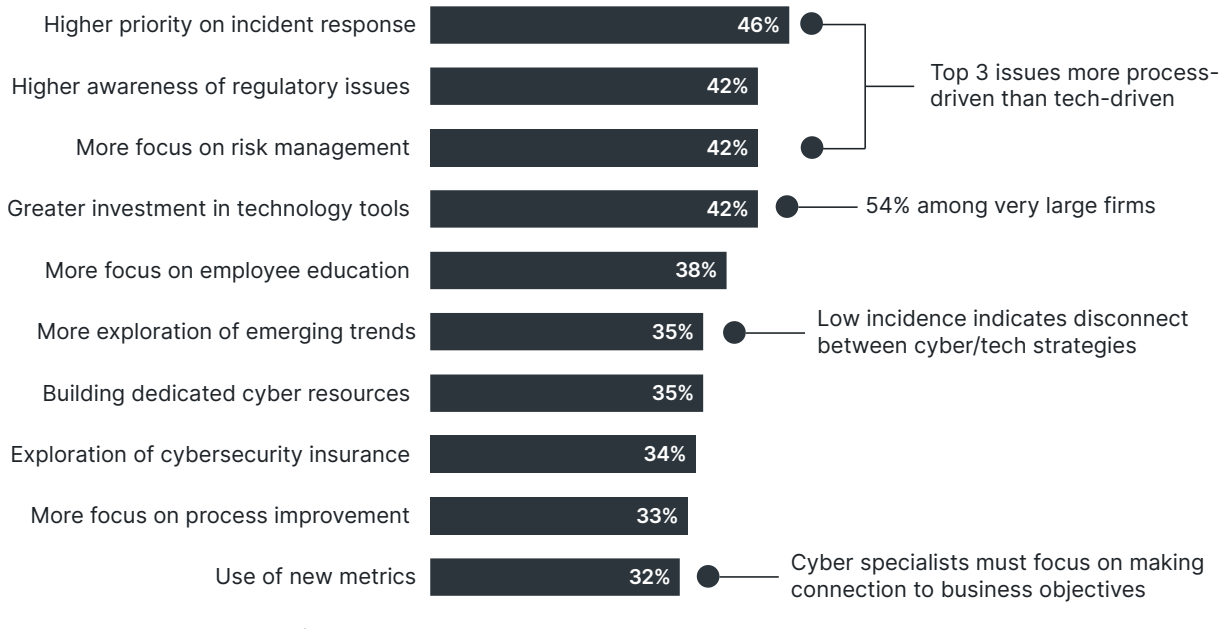
	Small (<100 employees)	Medium (100-499 employees)	Large (500-9999 employees)	Very Large (10000+ employees)
Emergence of generative AI	43%	**45%**	47%	52%
Variety of attacks	**48%**	42%	46%	49%
Privacy concerns	46%	41%	**49%**	47%
Reliance on data	41%	43%	45%	**55%**
Scale of attacks	46%	36%	43%	46%
Making business connection	38%	30%	41%	32%
Nation-state actors	34%	30%	40%	42%
Breadth of skills needed	35%	34%	36%	37%
Compliance with regulations	31%	35%	38%	38%

Source: CompTIA State of Cybersecurity 2025 | n=1025

Across the list of issues shaping cybersecurity plans, there is general consistency in the level of concern from one company size to another. However, the top concerns for each segment highlight the challenges associated with budgetary and resource scope. The smallest companies are most concerned with the variety of attacks, given that these firms have the fewest resources able to understand the threat landscape or respond to a wide range of malicious activity. Medium-sized firms are most focused on the emergence of generative AI, which can create new or expanded threat vectors but can also allow these firms to build on the limited specialists they may have on staff.

At the larger end of the scale, the concerns center on data. Large enterprises want to ensure they are handling privacy correctly, and the very large segment is motivated by their reliance on data, which is a critical component connecting the many pieces of a huge organization. For these companies, connecting cybersecurity strategy to data strategy is of utmost importance.

Many aspects involved in changes to cybersecurity approach



Source: CompTIA State of Cybersecurity 2025 | n=1026

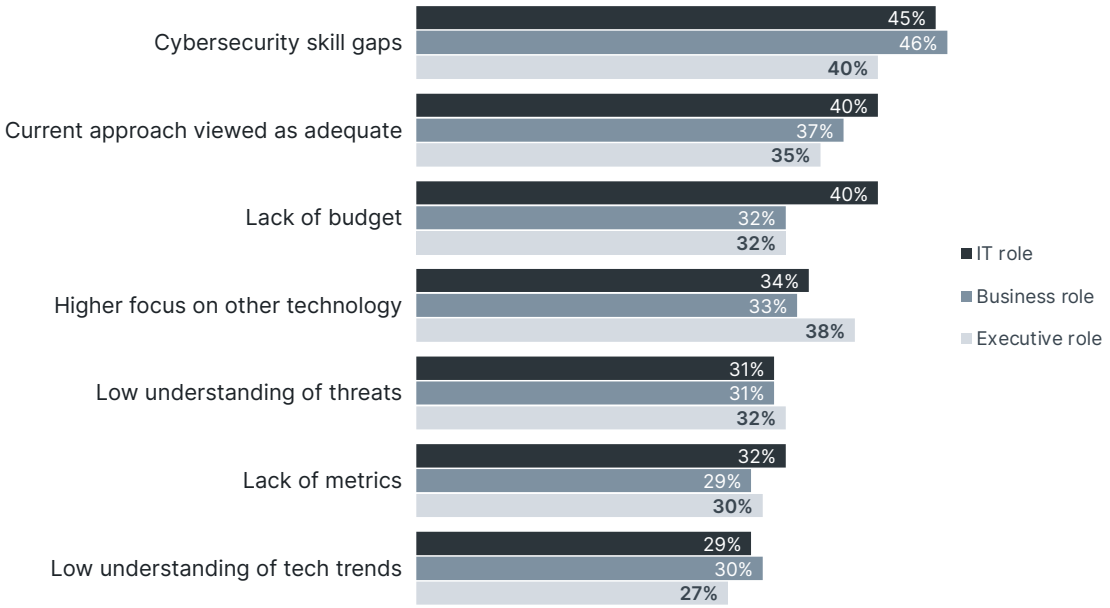
The many concerns that need to be addressed lead to many changes being made within cybersecurity implementation. Being satisfied with a cybersecurity posture does not mean standing still; it means that ongoing adjustments and adoption of new techniques are in line with organizational viewpoints. Even so, the changes many firms are making suggest further room for improvement and refinement.

Cybersecurity has traditionally been seen as a technical endeavor, a subset of the tools and skills that a company assembles for their broader technology strategy. The top changes being made, though, are process-oriented. Whether it is improving the incident response process, building a deeper understanding of the regulatory environment, or developing a more robust risk management approach, there is growing demand for individuals who understand the procedural aspects of cybersecurity.

Of course, there is still a strong technology component. New tools continue to be purchased—especially by the largest firms—and these tools need experts who can integrate them into a cohesive structure and efficiently apply layers of automation. AI continues to be the dominant emerging technology, but many companies leverage cross-functional teams to evaluate all new trends on the horizon, and these efforts likely still need additional cybersecurity oversight.

The least-implemented change is the development of new cybersecurity metrics, which provides another piece of evidence that executives may be feeling fatigue around cybersecurity rather than being convinced that investments and operations are properly serving the business. As technology has become a strategic driver instead of a traditional cost center, there has been increased demand for technology professionals to connect their efforts to corporate success and growth. The same holds true for cybersecurity, with the added challenge that cybersecurity activities are often protective or preventative, not ingredients for higher revenue or product expansion.

Overcoming cybersecurity challenges requires communication across functions



Source: CompTIA State of Cybersecurity 2025 | n=1026

The theme of connection between cybersecurity efforts and business imperatives can also be seen in the list of challenges companies face in pursuing a cybersecurity agenda. Some challenges, such as the need for better threat understanding or the lack of metrics, are shared evenly across IT staff, business staff, and executives. For the most part, though, executives take a lower view of cybersecurity hurdles, especially when compared to IT staff. If technical professionals are concerned about skill gaps or budget shortfalls, they need to find ways of framing these risks in terms executives will understand.

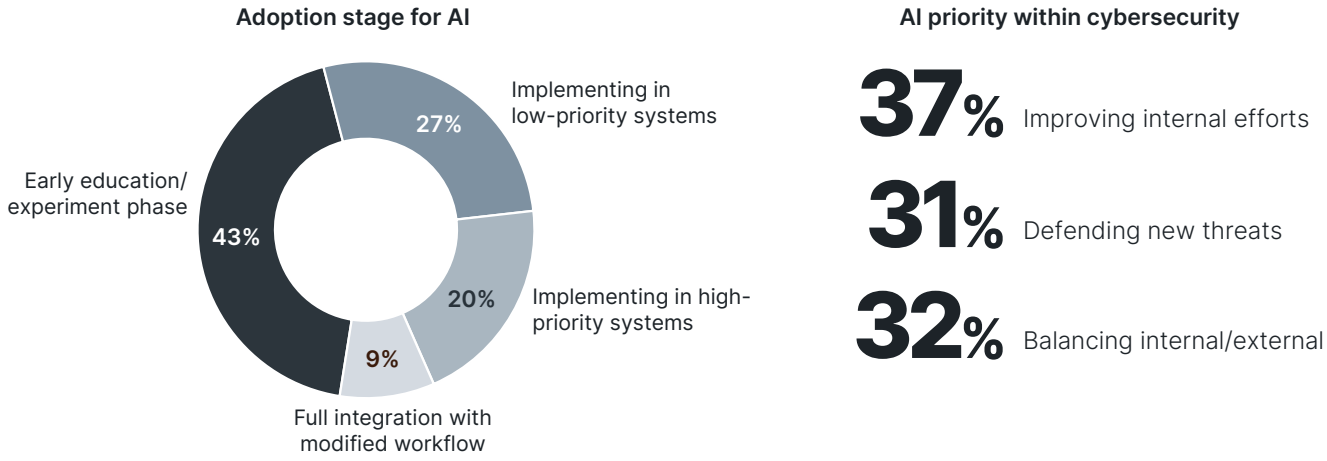
The one area where executives feel more strongly than both IT professionals and business staff is in placing more of a priority on other technology initiatives. Of course, executives may not view this as a challenge per se. Their viewpoint may be that other technology deserves more attention if it has the potential to be revenue-generating. Cybersecurity will always have a return-on-investment challenge compared to technology that can boost productivity or shorten development cycles, but it is imperative that security considerations are taken into account when evaluating new tech implementations.

In addition to skill gaps, budget constraints, and threat understanding, one overriding challenge of cybersecurity is the many different facets that must be considered in building a comprehensive strategy. The days of building a secure perimeter around standard system assets are in the distant past, and cybersecurity has splintered into many distinct focus areas. As businesses continue to transform their operations and workflow, the topics of AI, operational technology, and data are the most pressing issues alongside traditional network and endpoint security.

2 AI: Transforming Operations and Defense

Artificial intelligence continues to dominate technology discussions, with businesses emphasizing AI fluency among their workforce and examining their workflow to understand opportunities for automation. Cybersecurity professionals have dual concerns when it comes to AI. As with the rest of the workforce, they want to use AI to improve their daily operations. In addition, they must also become informed about the ways that AI changes the threat landscape by creating new threat vectors and changing the quality and quantity of previous threats.

Organizations are largely in early stages of adoption with AI

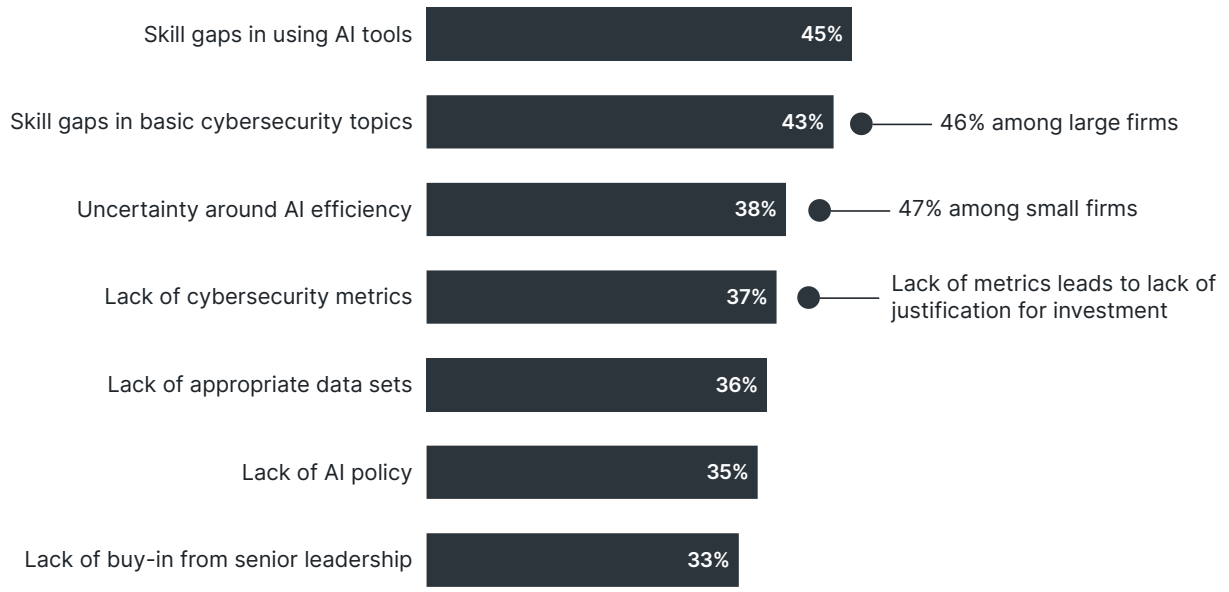


Source: CompTIA State of Cybersecurity 2025 | n=1026

Given all the hype around AI, it is easy to lose sight of the fact that companies still go through an adoption curve, where new technology must be integrated into digital architectures and workflows that have become incredibly complex. In fact, the higher potential a technology has to be disruptive, the longer the adoption cycle will likely be. This trend is borne out in CompTIA's data, where 70% of firms place themselves in an early education phase or a stage of testing AI implementation on low-priority systems. That number actually may be low, as CompTIA research has historically found that companies overestimate their capabilities in early days of technology adoption. For example, while AI is rated as the lowest proficiency among technical topics, 52% of companies rate themselves as having high capability. This is at odds with the adoption numbers, and there will undoubtedly be new viewpoints on capability as new challenges arise in implementation.

From a cybersecurity standpoint, there is a relatively even split between those organizations focused on internal improvements and those focused on defending against new threats. Smaller firms skew toward internal efficiency, likely seeking to make the most out of limited resources, while larger firms tend to take the balanced viewpoint, possibly assuming that their specialists in each area will leverage AI appropriately. There is a slight lean toward defending against new threats among companies claiming to be satisfied with their security approach, suggesting that these firms may be less anxious about investing in internal efforts.

Skill gaps lead the list of challenges in using AI for cybersecurity



Source: CompTIA State of Cybersecurity 2025 | n=1026

What could help organizations accelerate AI adoption? There's no surprise to see AI skills at the top of the list of challenges. For the past three years, there has been intense focus on how AI will affect the workforce, including speculation on new job roles that may be created or the level of AI fluency required by employees in all career fields.

However, all this conjecture overlooks the layered nature of skill-building. As with previous emerging technologies, there are few situations where new standalone skills in AI are currently critical components of job responsibilities (these situations are mostly concentrated in software development). For the vast majority of workers, AI skills are an extension of the foundational knowledge needed to be successful.

This is evident in the next challenge on the list. Following closely behind AI-specific skills, companies need improvement in foundational cybersecurity skills. These skills not only ensure that cybersecurity approaches are following best practices, they also provide the necessary input for training AI systems properly. One downside of AI tools is that they can act as a black box, obscuring decision-making algorithms and complicating optimization. Without the prerequisite skills in cybersecurity practices, it becomes more difficult to fully implement AI that meets organizational objectives.

CompTIA's AI Framework provides a model for the type of skill-building needed in the AI era. The different elements of the AI Framework cross over the different job families making up the tech workforce. Cybersecurity professionals will certainly require both depth and breadth in AI Security skills, but they will also require some level of skill in the other domains of AI Interaction, AI Systems, AI Data Analytics, AI Architecture, and AI DevOps.

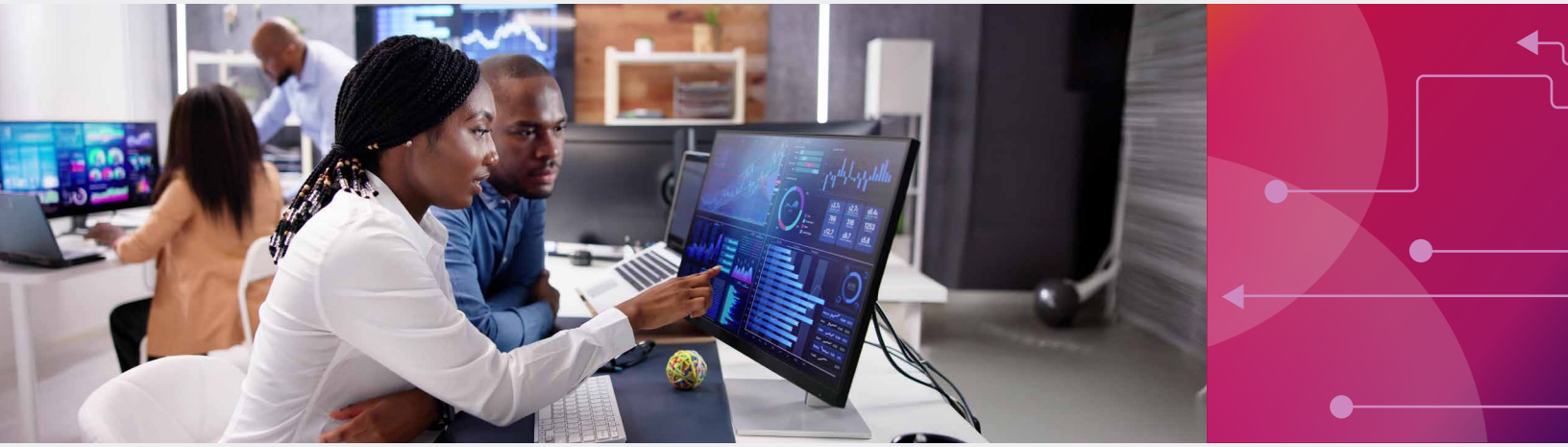
How AI Is Changing Cybersecurity

As with any new technology, the primary question around AI is how it will appear in enterprise use cases. After three years of generative AI in the market, there is still tremendous focus on individuals using chat tools to find information, create content, and perform tasks. There is slow movement toward integrating AI into workflow that can scale to teams and organizations, but that integration is the key that will unlock massive productivity boosts.

As companies find ways to build AI into their system architecture, the early indications suggest that use cases will follow a similar pattern to skill development: New activity will be built on a foundation of existing practices. AI is a tool that is most effective with the proper guidance, and that guidance comes from a strong knowledge of fundamentals and well-established workflows. The initial intersections of AI and cybersecurity demonstrate this hierarchical state of affairs.

Supercharged Attacks

One of the realities of cyberattacks is that there is no need for something new if the old attacks are still effective. The nature of generative AI means that attackers will explore new ways to attack systems, by influencing the input of LLMs or the behavior of algorithms. The immediate concern, though, is attackers using AI to make existing attacks more formidable. A group of New York University researchers recently built an AI system that performs all phases of a ransomware attack, and AI-generated deepfakes are being used regularly for social engineering.



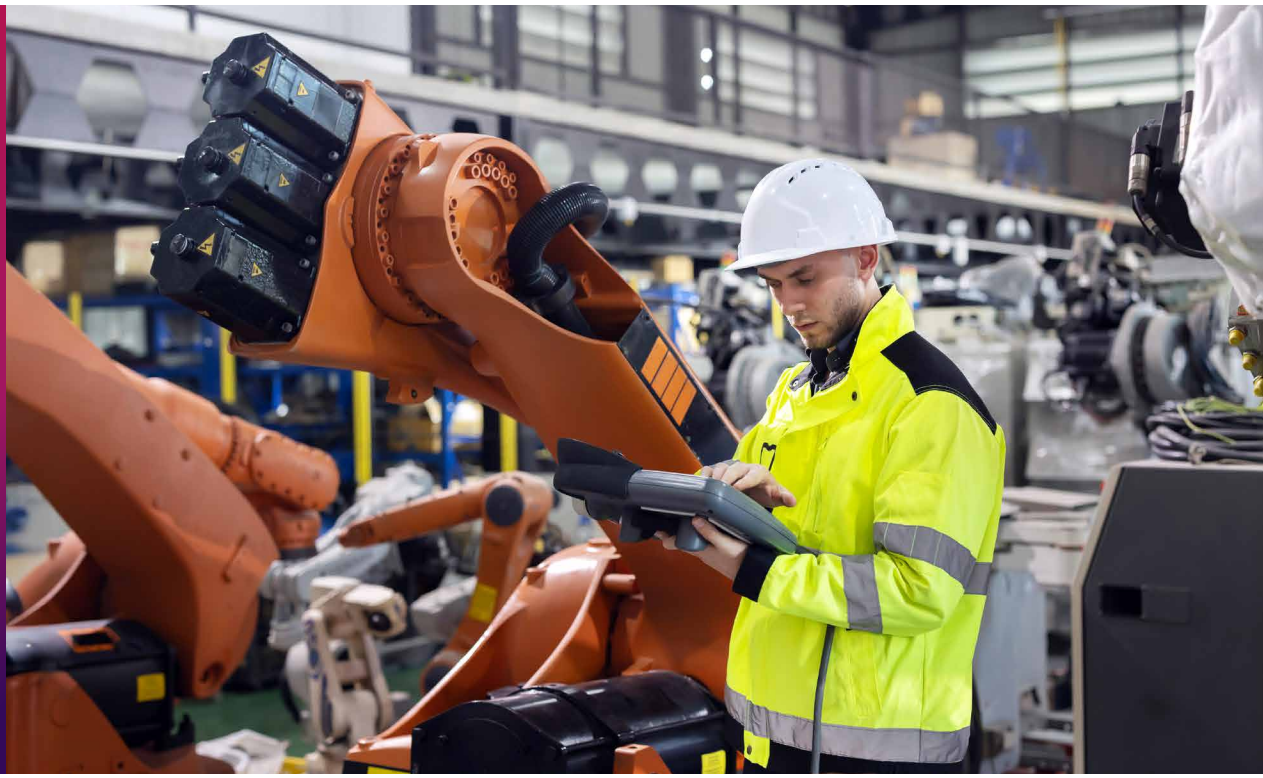
Threat Detection

With so many types of threats to contend with, cybersecurity professionals rely on network analysis and pattern recognition to discover malicious behavior. These activities are typically driven by rules defined by the cybersecurity team, and AI can enhance capabilities by learning from past activity and flagging new suspicious that go beyond a strict set of rules.

Operational Automation

Without a doubt, cybersecurity has a tremendous amount of complexity. For years, cybersecurity professionals have worked to organize that complexity with Security Information and Event Management (SIEM) tools and scripting. AI can accelerate automation efforts, allowing cyber specialists to focus on strategic work. Ultimately, though, automation and threat detection—along with other cybersecurity activities— require some degree of expertise for training and ongoing oversight.

3 Operational Technology: Merging Digital and Physical

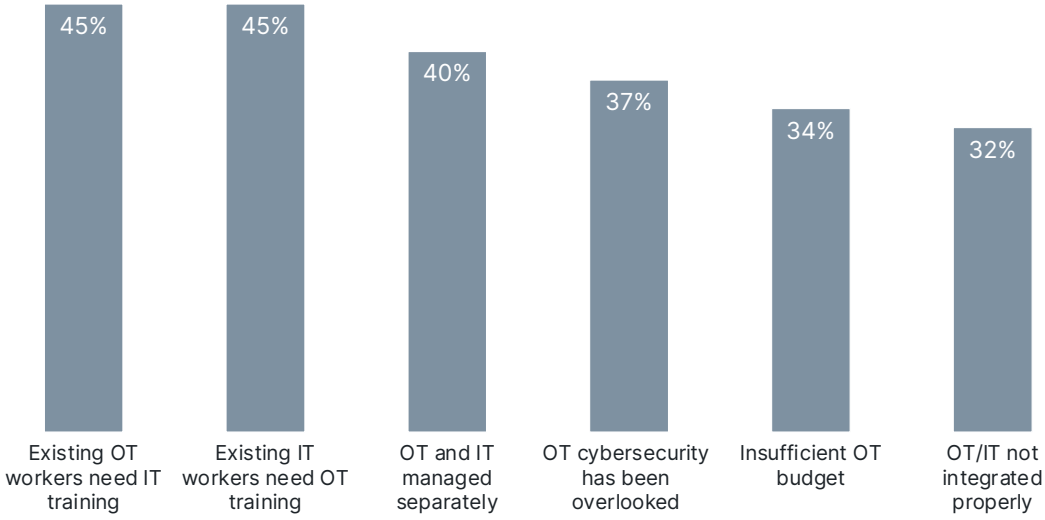


Digital transformation is not only affecting IT systems; it is also impacting physical infrastructure. The conversation around Internet of Things (IoT) has largely become a conversation around operational technology (OT), as digital sensors and controls have moved beyond niche applications to become embedded in the real-world assets of an organization.

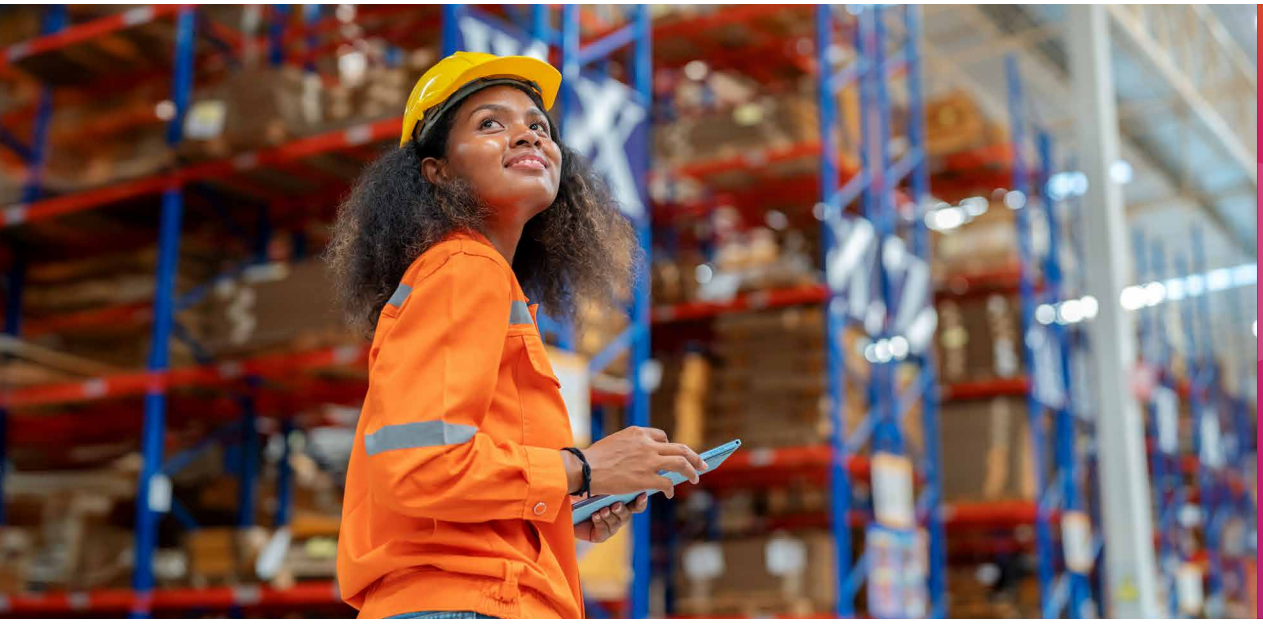
The field of OT has roots in critical infrastructure such as power grids or water plants, as well as manufacturing facilities. In these industries, the introduction of digital systems introduces a substantial threat to safety and core operations. The technology used by OT teams is very different from traditional IT, with components such as programmable logic controllers (PLCs) and frameworks such as supervisory control and data acquisition (SCADA). Securing this technology obviously requires different knowledge and a new approach.

OT is now reaching far beyond these critical infrastructure examples, though, as businesses digitize their building management functions or their physical security systems. More and more organizations are growing concerned about the vulnerability of their OT architecture, with 58% of firms saying they have a high focus on OT and 36% saying they now have a moderate focus.

OT/IT integration is imperative for robust cybersecurity posture

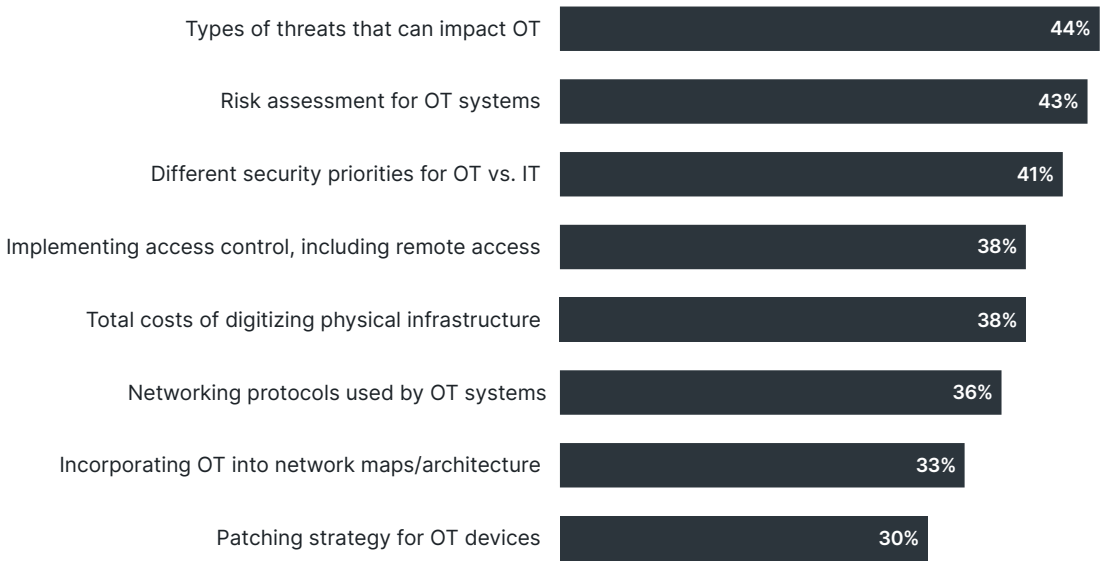


Source: CompTIA State of Cybersecurity 2025 | n=1026



The most significant challenge in securing newly digitized OT is that the OT and IT functions have traditionally been managed separately. This makes perfect sense, since there has traditionally been far less overlap. Today, though, the two sides need to be talking much more frequently and speaking each other's language. This is why organizations cite equal training need for both OT and IT workers in trying to build a comprehensive strategy.

Wide range of topics must be understood better to properly secure OT

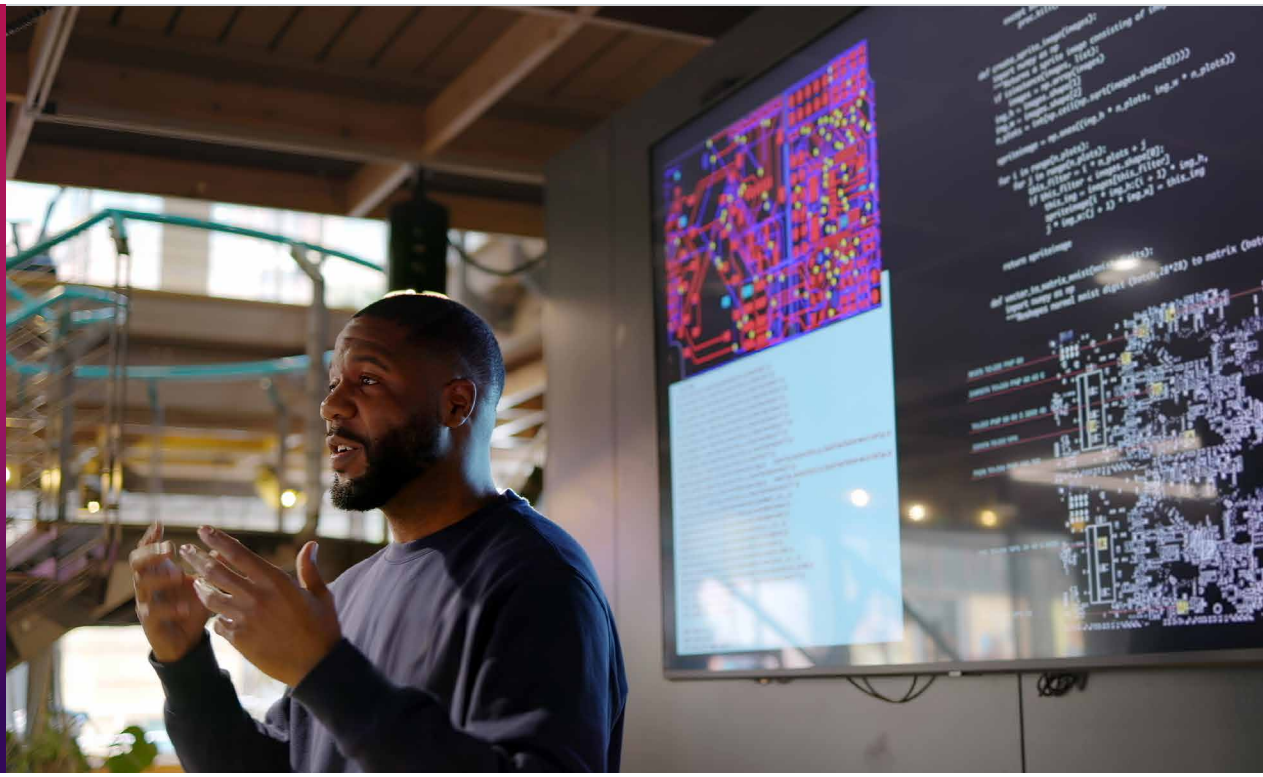


Source: CompTIA State of Cybersecurity 2025 | n=1026

The list of desired training topics shows that information clearly needs to flow both ways. The OT team must educate the cybersecurity function on the threats that should be added to a threat matrix. Access control built by IT must extend to OT systems. OT components must be added to network maps to provide a holistic view of operations and attack surface.

Ultimately, OT and IT still have to describe their risks and operations in terms that make sense to the business. This means jointly deciding on priorities and mitigation plans so that decision makers can sign off on a strategy that best serves the needs of the organization. Presenting a full suite of options requires detailed technical training for specialized staff and risk analysis capabilities for team leads and managers.

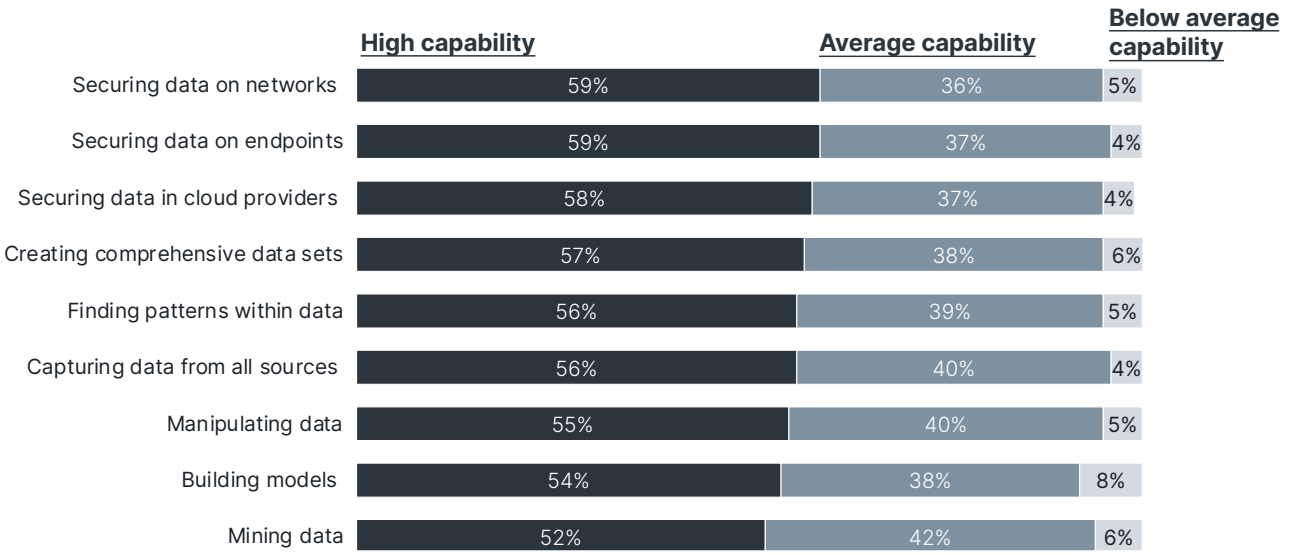
4 Data: Guarding Corporate Knowledge



The importance of data has steadily increased over the past decade. Starting with the push to improve analytics proficiency for forecasting and market insights, companies now need to build extensive, organized datasets for training AI tools. Data is abundant as businesses have been digitizing operations, but that data serves no purpose if it cannot be properly managed and secured.

Data security, along with application security, has become a dedicated practice in a cloud-based economy. The dissolution of the secure perimeter means that both data and applications now require dedicated focus. However, while applications can be built securely by either an internal team or a vendor, data demands much more of a separate process.

Less than 6 in 10 companies have high capability across data activities



Source: CompTIA State of Cybersecurity 2025 | n=1026

Data passes through many stages as it flows through an organization, from creation by various sources to storage/manipulation and finally analysis. Security at every point is the highest priority for many firms, and accordingly data security is the area where the most companies rate themselves as having high capability. Small and medium-sized businesses lag behind large and very large enterprises in data security capability—a dangerous position in a world where cybercriminals are increasingly adept at finding weak links.

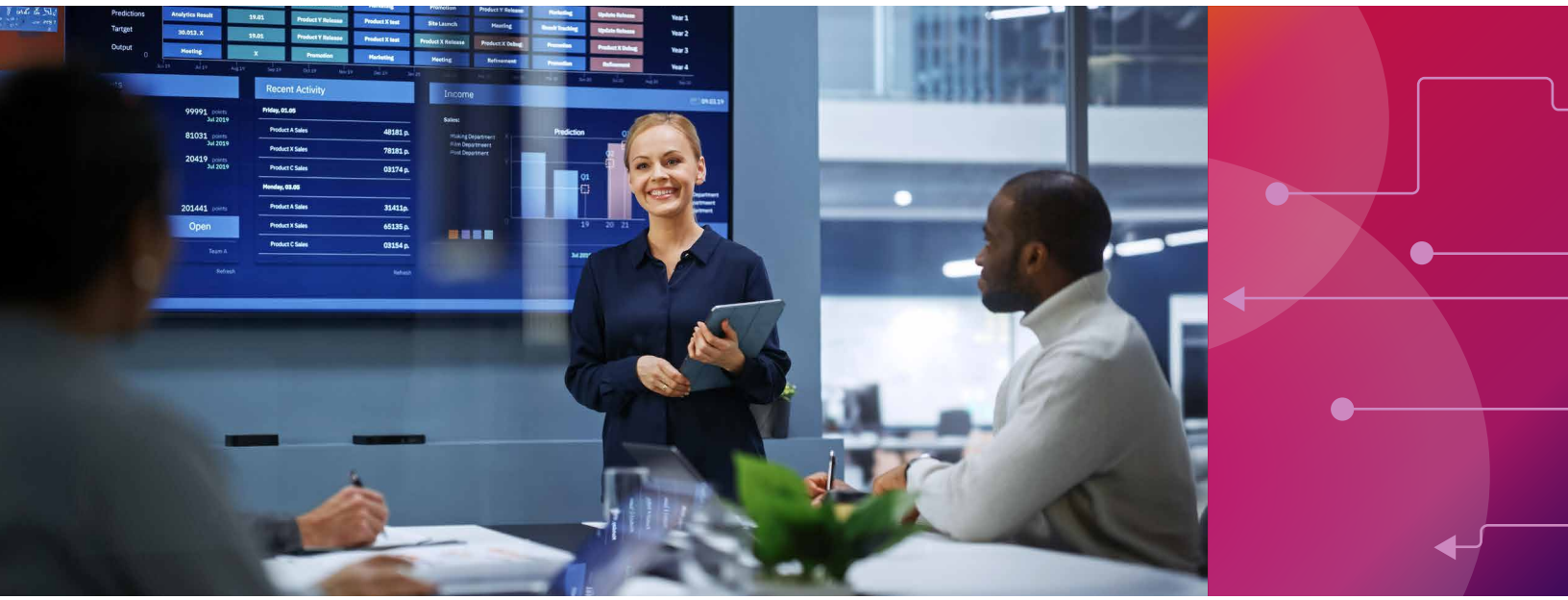
In building or improving capability, companies are often creating dedicated teams or individuals for handling data activities. This is most common for data security, where 66% of companies have dedicated employees, compared to other high-profile activities such as database administration (60%) and data analytics (58%).

Challenges in data security include comprehensive understanding and organizational processes

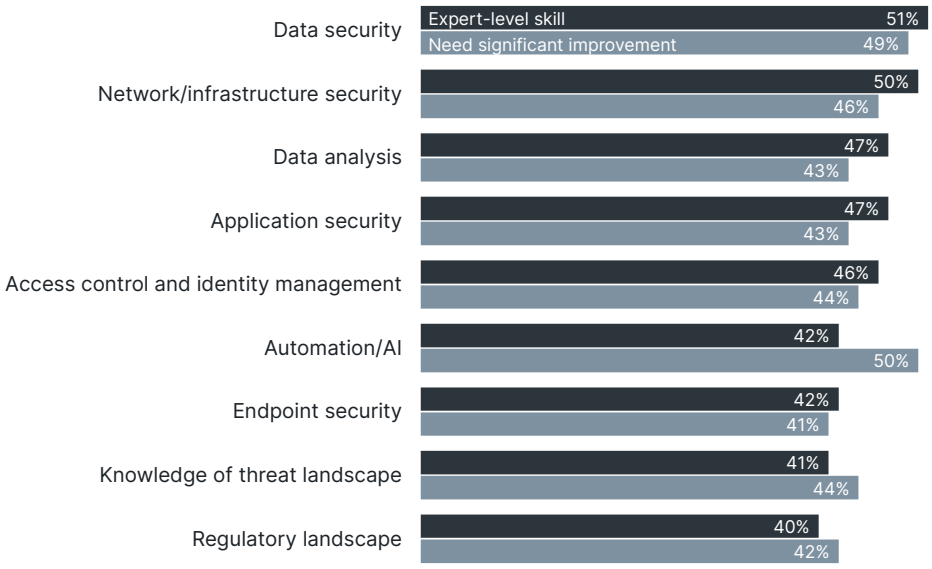
1. Awareness of all data locations
   - Data silos within departments make it difficult to understand where all corporate data resides
2. Decision processes around storage
   - Deciding which data should be stored and the storage duration greatly impacts architecture
3. Awareness of regulations around data
   - Different regulations across states or countries can complicate compliance requirements
4. Prioritizing data for disaster recovery
   - Classifying data according to priority shapes disaster recovery strategy and risk assessment
5. Observability of data in various locations
   - Low visibility across asset classes leads to low confidence in appropriate security plans

Source: CompTIA State of Cybersecurity 2025 | n=1026

One key way that securing data differs from securing other parts of IT architecture is that data is an asset in which the entire organization has direct interest. Business units may not be concerned with endpoints, applications, or backend infrastructure beyond function and availability, but they typically have more pressing demands around data, including accessibility and impact on decisions. For this reason, data security relies on building consensus throughout the organization on how data is collected, managed, and prioritized. This consensus then drives security strategy.



Low correlation between skill assessment and desired improvement suggests need for deeper understanding of knowledge, skill, and task



Source: CompTIA State of Cybersecurity 2025 | n=1026

Aside from the focus areas of AI, OT, and data, there remain many aspects of traditional cybersecurity that require improved capability or process as they evolve. As in previous years, there is a low correlation between the assessed level of skill in a particular area and the desired level of improvement. Automation and AI stand out as the biggest disconnect, but the small gaps in other areas such as data security, network security, and endpoint security point to a need for more granular assessment of current capability and more definition around how subject matter expertise is connected to daily operations.

5 Managing Risk and Handling Incidents

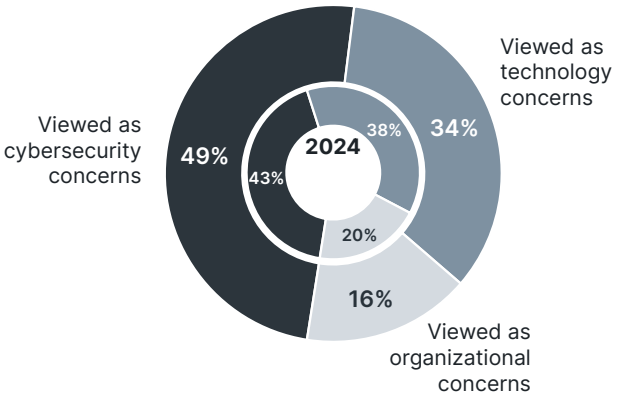
Two of the common themes emerging throughout this report and previous State of Cybersecurity reports are the focus on risk management and the need for metrics. These two themes tie together, as cybersecurity professionals need to help lead the risk management activities at their organization, then provide the appropriate measurements proving that risks are being managed.

Risk management is critical because it defines the goals and constraints of a cybersecurity strategy. As cybersecurity has rapidly grown in complexity, businesses have realized that there is no such thing as perfection (or if there were, it would be too costly to implement). With so many angles to consider and with the goal of zero incidents being unrealistic, risk management allows decision makers to evaluate and quantify the threats to the business, then determine the best investments for mitigation and response.

The good news is that most organizations claim to perform some style of risk management. Over half of the companies surveyed (56%) say that they are using a formal risk management framework, such as the NIST Risk Management Framework (RMF) or the IRGC Risk Governance Framework. Another third say that risks are assessed informally. This provides the groundwork for a modern cybersecurity strategy that accounts for those threats that are deemed most relevant.

Risk analysis and mitigation should be an organization-wide process

Viewpoints on risks identified through analysis



Top elements involved in risk analysis

45% Use of cloud computing

45% Technology procurement

44% Operational technology (OT)

39% Data classification

38% Data ownership

Source: CompTIA State of Cybersecurity 2025 | n=1026
CompTIA State of Cybersecurity 2024 | n= 525

The issue, though, is the way that risk mitigation appears to be executed. Once risks are identified, the vast majority of businesses seem to hand these concerns to the technology function, with 49% specifically viewing the cybersecurity function as responsible. Even if this is a statement on ownership and there is organization-wide collaboration in mitigating risks, the mindset may be limiting, and the situation has shifted more toward technology/cybersecurity ownership in the past year.

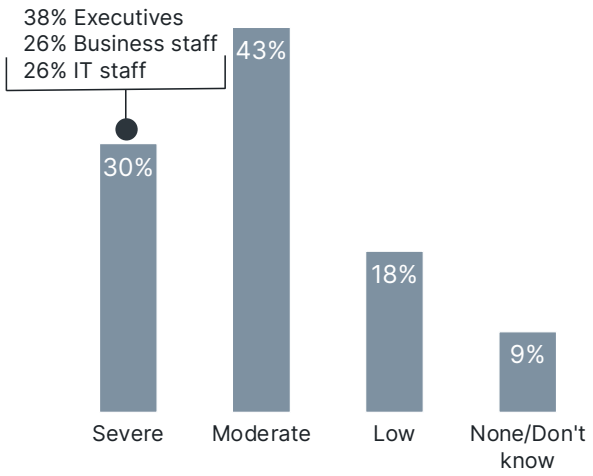
A review of the operational elements that commonly rise to the top in risk analysis highlights the error in viewing risks as technology-centric. Cloud computing implementation may be driven largely by an infrastructure team, but there is a significant financial component that many businesses still struggle with. Technology procurement has shifted from the wild west days of shadow IT toward more technology oversight, but there is still the most flexibility when business units have some degree of autonomy. Data classification and ownership drive technical activity such as storage architecture and disaster recovery, but the entire organization needs to weigh in on these issues. The technology/cybersecurity function should take the lead on risk management activities, but the entire process should be viewed as an organizational concern.

Of course, part of identifying and classifying risks is realizing that cyber threats remain very real and still happen with alarming regularity. The benchmark Cost of a Data Breach Report from IBM/Ponemon reports that the average cost of a breach in 2025 is $10.22 million for U.S. companies ($4.44 million globally). These costs include the time and effort to contain a breach and recover, potential regulatory fines or legal costs, and reputational damage. To no surprise, AI features prominently as a new technology that businesses have yet to fully understand, as the report finds that 97% of AI-related security incidents occur in organizations where there are no defined AI controls. As companies encourage the use of AI among their employees, they are opening the door for cybersecurity incidents if they have not thought through the ramifications.

Although endpoint security is a well-established practice, it may rank lower on the list of assessed capabilities because endpoint incidents remain so common. Lost/stolen devices and malware on devices are the top two incidents reported by companies in CompTIA's sample. The next three incidents target another well-established practice in network security; malware in backend infrastructure and unauthorized infrastructure access rank just ahead of ransomware.

OT/IT integration is imperative for robust cybersecurity posture

Impact of cybersecurity incidents



Elements of incident response

1. New software purchased
2. Technical staff diverted from work
3. Technical staff working overtime
4. New hardware purchased
5. Business staff disrupted
6. Communications to customers
7. Purchasing fraud/credit services

Source: CompTIA State of Cybersecurity 2025 | n=1026

Nearly three in four companies report the impact of cyber incidents in the past year as being severe or moderate, but there is an interesting division between executives and the rest of the workforce. Executives are far more likely to rate incidents as having a severe impact, and the typical elements involved in incident response may provide a reason for this viewpoint. Three of the top seven elements involve some sort of purchase—new software, new hardware, or fraud/credit services for customers. To business staff, it may seem that the incident had minimal impact on daily operations. To IT staff, it may seem that the technical issues were resolved in a reasonable fashion. To executives, there is a direct impact on the bottom line.

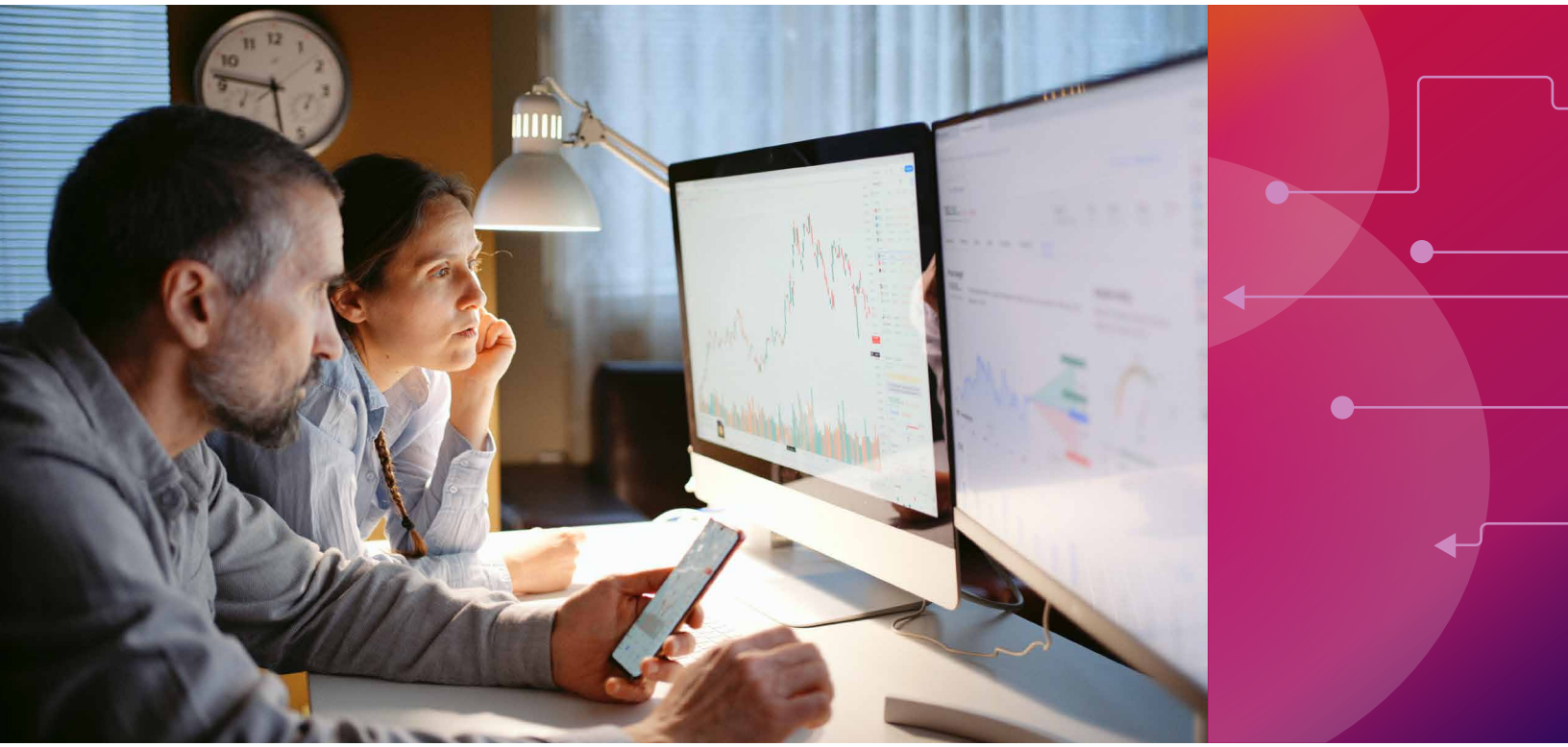
Given a similar disconnect around lack of budget being a challenge for cybersecurity operations, this continues to drive home the point that cyber professionals must find better ways to communicate the total scope of a cybersecurity strategy. It is not enough to say that an ounce of prevention is worth a pound of cure. They must have historical data to prove this point or statistical models that make the case. This highlights another area where cybersecurity professionals may need to build skills: data management and analysis.

Need for understanding of threats is relatively consistent across all formats

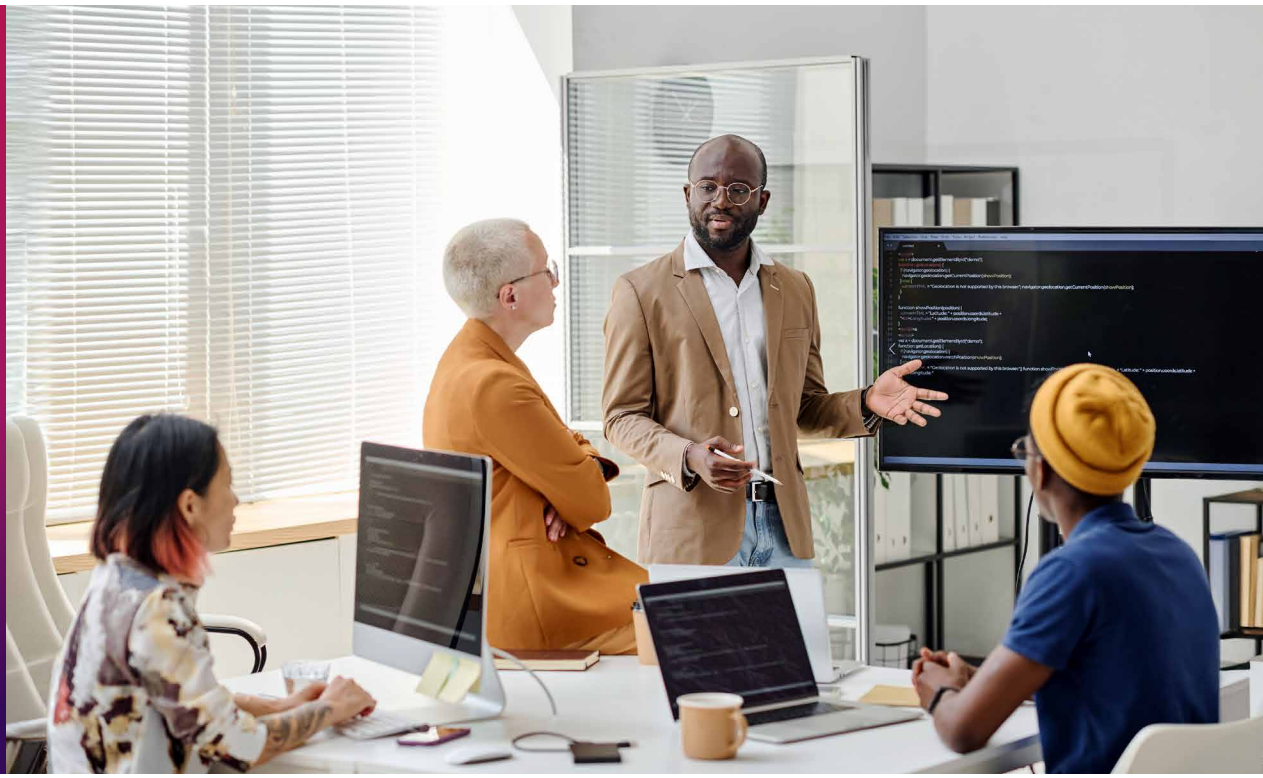
Source: CompTIA State of Cybersecurity 2025 | n=1026

Education is a large part of the communications that need to happen. This is true at the executive level but also across the rest of the workforce, as the cybersecurity team seeks to inform staff of pertinent threats and raise awareness on appropriate behavior. Just as there are many aspects of an attack surface to consider, there are many threats that cyber criminals use to gain information and disrupt systems.

The list of threats also demonstrates the potential of AI in this space. There is not an entry for "AI attack" on this list because AI can drive the creation or efficiency of any of these threats. As AI becomes a more established part of the enterprise technology stack, there will doubtless be new forms of attack that cybersecurity professionals must contend with. For now, their hands are full dealing with existing threats that are growing much more powerful.



6 Developing a Skilled Cybersecurity Team



There are clearly many factors to consider when building and executing a strong cybersecurity strategy. The overwhelming threat landscape, the impacts of digital transformation, and the shifting regulatory environment all add up to create massive challenges for business leaders trying to determine the best approach.

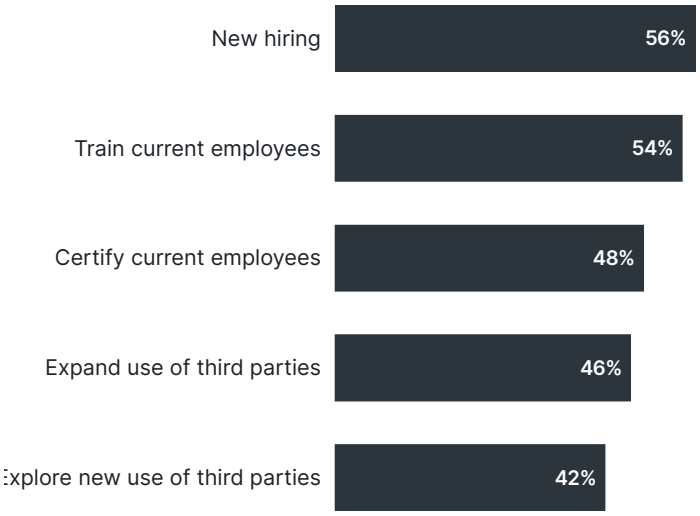
In the face of all these complications, the uptick in satisfaction with current tactics may be understandable, as leaders begin to feel that they have already placed significant effort into cybersecurity transformation and have now built a reasonable strategy. Indeed, the feeling that the current approach is "good enough" is the second-greatest challenge in improving execution.

However, it is worth returning to the list of challenges to further discuss the top hurdle. Even with more positive feelings around cybersecurity, the need for skills is the most pressing problem according to executives, business staff, and IT staff. Even in a tight labor market, demand for cybersecurity skills is difficult to solve. CompTIA's Cyberseek tool, developed in partnership with NIST and Lightcast, reports over 514,000 cybersecurity-related job postings between May 2024 and April 2025, compared to nearly 470,000 from the prior year.

One of the underlying reasons that demand remains high is the way that companies are attempting to build cybersecurity teams. CompTIA's IT Industry Outlook 2025 found that cybersecurity is the field where the fewest companies with hiring plans are targeting early career candidates. This may stem from the previous method of creating dedicated cybersecurity employees, which was to select mid-career infrastructure professionals and direct them to specialize.

Skills-based approach needed for hiring and training to fill range of skill gaps

Options being considered for skill improvement



Skills that require improvement

	Significant/moderate improvement needed (NET)
Network/infrastructure security	97%
Data security	97%
Application security	96%
Identity management	96%
Regulatory landscape	95%
Endpoint security	95%
Data analysis	95%
Automation/AI	95%
Knowledge of threat landscape	94%

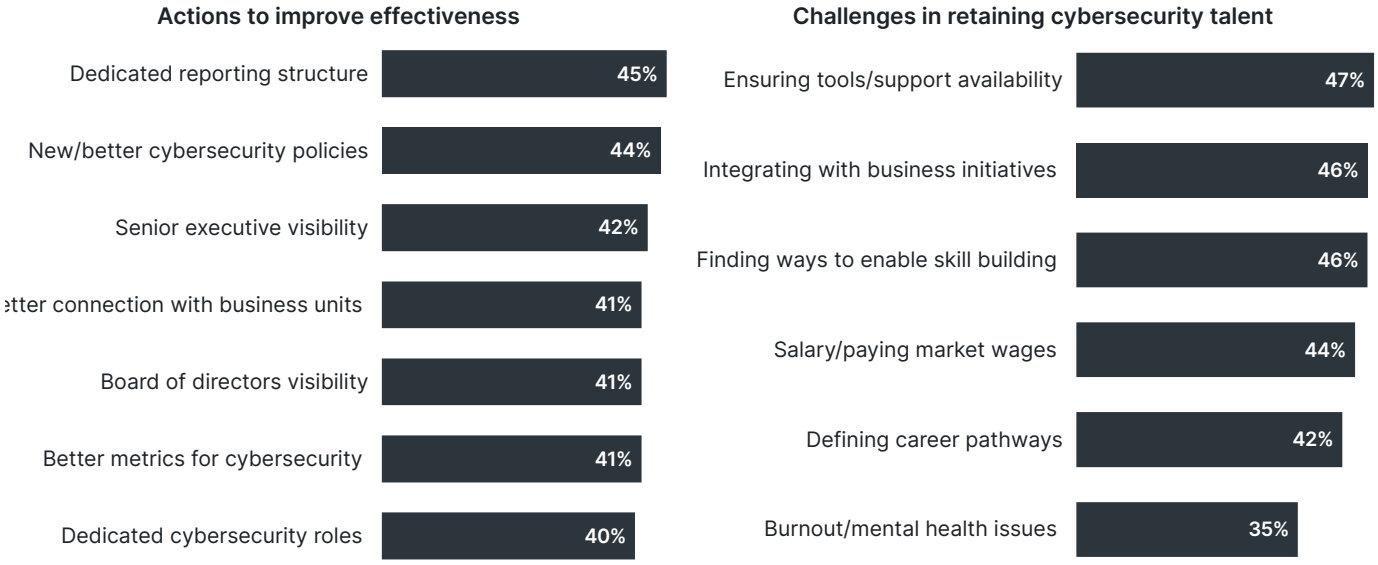
Source: CompTIA State of Cybersecurity 2025 | n=1026

That mindset is not sustainable now, especially with the wide range of skill gaps that need to be filled. Mid-career employees may have depth of specialization, but there are not currently enough to meet demand. Companies must give more consideration to building a pipeline of cybersecurity talent, through a combination of hiring early career specialists and providing internal training to allow for career growth or reskilling opportunities.

This multi-pronged approach requires further refinement to the skills-based methodologies many companies have begun adopting. The first area to refine is skill assessment. Along with the low correlation between current assessment and desire for significant improvement, the tight grouping of skills that require significant or moderate improvement points to a need for better understanding of the skill landscape.

Beyond assessments, businesses must understand how to ensure they are actually hiring or developing the skills required. Industry-recognized certifications play a vital role here, providing more granular skill validation than typical four-year degrees and proving adherence to best practices and industry standards after completion of internal training.

Effectiveness and retention must be addressed to ensure a productive team



Source: CompTIA State of Cybersecurity 2025 | n=1026

Bringing the proper talent on board is only the first step, though. In a high-pressure field such as cybersecurity, there must be a focus on getting the most productivity out of these rare resources and ensuring that they remain motivated. There are several actions companies are exploring to improve the effectiveness of their cybersecurity team, ranging from organizational structure to enforceable policies to a communication flow that ties cybersecurity efforts to business success. For motivation and retention, the total cost of cybersecurity comes into play as companies must provide the proper toolset and skill development opportunities along with competitive salary and benefits.

In some ways, the field of cybersecurity is the same as it always was: cybersecurity efforts must ensure confidentiality, integrity, and availability. That simply stated objective should not lull organizations into a false sense of confidence. The drive to push the envelope in technology adoption combined with the ever-changing nature of attacks and insider threats leads to a discipline that is hard to quantify but vital to organizational health. As businesses scramble to develop the skills needed for AI, OT, and data security, the next trend—and the next threat—always looms on the horizon.

Methodology

This quantitative study consisted of an online survey fielded to business and IT professionals involved in cybersecurity during Q3 2025. A total of 1,026 professionals based in the United States participated in the survey, yielding an overall margin of sampling error at 95% confidence of +/- 3.1 percentage points. 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

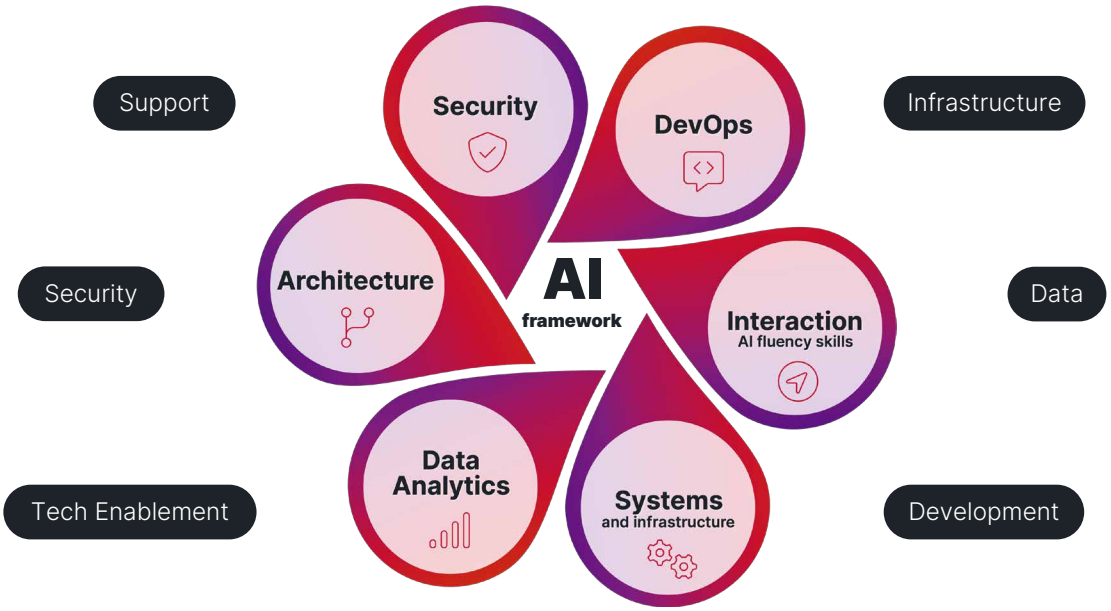
The Computing Technology Industry Association (CompTIA) is the world's leading information technology (IT) certification and training body. CompTIA is a mission-driven organization committed to unlocking the potential of every student, career changer or professional seeking to begin or advance in a technology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

Appendix A

Mirroring the pattern of prior waves of disruptive technologies, artificial intelligence (AI) will transform the workplace on multiple fronts. From automating tasks to augmenting human effort, AI will simultaneously create, reshape, and displace job roles and functions. Organizations face new challenges in navigating the complexities of a rapidly changing future of work.

CompTIA's tech jobs taxonomy defines the job families, job roles and underlying detail of the tech workforce. CompTIA's AI framework extends this approach. As an enabling technology, AI, and the skills that accompany it, will permeate every component of the framework.

AI skill domains intersect with broader job families



Source: CompTIA

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.