ASIS INTERNATIONAL | SECURITY ISSUES RESEARCH

UNDERSTANDING THE EVOLVING ROLE OF SECURITY

2025 SECURITY TRENDS RESEARCH

Sponsored by

Resolver.
A KROLL BUSINESS

CONTENTS

ASIS INTERNATIONAL

Advancing Security Worldwide®

ASIS International would like to thank Resolver for their sponsorship of this research.

Resolver.
A KROLL BUSINESS

KEY FINDINGS

SECURITY IS GETTING MORE INTEGRATED INTO THE BUSINESS.

For years, the security function has worked to show that its mission of protecting assets goes well beyond surveillance cameras, guard patrols, and access control, and this research shows that work is paying off. Both in perception and actual practice, more organizations have shifted to see security as a key business enabler rather than a cost center. This trend has many important implications for security, including being a part of strategic decisions, and, importantly, being able to obtain needed resources.

DESPITE THE PROGRESS, THERE CONTINUES TO BE ROOM FOR GROWTH.

While the findings on security's role within organizations are trending in the right direction, there is still plenty of room for growth. There is a small but meaningful perception gap between what an organization's leaders think and how security professionals see security's role. In particular, most security functions could do more to determine the department's return on investment and in building its influence in the organization's overall risk practice.

INTEREST IN HOW ARTIFICIAL INTELLIGENCE (AI) CAN IMPROVE SECURITY IS HIGH, AND THERE IS GROWING USE OF AND CONFIDENCE IN AI.

Incorporating AI into physical security technology systems, especially video surveillance, has made security one of the vanguard sectors of AI professional use. More than half of security professionals use AI in some professional capacity, and most of them see that use as beneficial. Interest in learning more about AI remains high.

SECURITY DEPARTMENTS THAT ARE MORE STRATEGIC, MORE HIGHLY INVOLVED IN RISK MANAGEMENT, ARE RESOURCED ADEQUATELY, AND HAVE BEGUN USING AI TOOLS ARE MORE LIKELY TO BE REACHING DESIRED SECURITY OUTCOMES.

It should not be a surprise that security professionals who report that their security departments operate on strategic levels, such as by working to be a business enabler rather than a cost center and by integrating deeply into the organization's overall risk management process are also more likely to report that their organization's ability to protect its assets is improving. Likewise, making investments in security, including in AI, has similar benefits.

POSITIVE CHANGES IN SECURITY'S PERCEPTION WITHIN THE ENTERPRISE

Security departments have long had a perception problem. Colloquially it's been called the "guns, guards, and gates" problem, as in those areas—throwing in surveillance for good measure—are what security is primarily responsible for. Security has also been described as the organization's rule givers and rule enforcers: When security showed up in someone's office, the initial thought was, "Oh no, what did I do?"

More recently, there has been a rapid surge in board and executive suite interest in cybersecurity. In many cases this has overshadowed or even diminished other forms of corporate security, despite the fact that the functions are intrinsically linked.

The ASIS Foundation has produced two research studies in the last few years highlighting this perception problem. In *The State of Security Management,* researchers said security was plagued by parochialism—that it had a narrow focus in the organization and even within different security disciplines.

The ASIS Foundation's *The Influence of Security Risk Management* report was even more stark, including several key findings that described security's limited capacity to make organizational impacts:

- Security is a technical specialized activity, resulting in lower influence than broader generalist activity managers.
- Security is seen as an operational risk concern, with limited strategic implications.
- Security professionals need to engage better with corporate decision makers.
- Security as a brand lacks professional respect compared to traditional professions.

These studies informed the creation of the survey detailed in this report. The research attempted to see if security is making any headway in redefining its role within organizations, and there are clear indications that security is in fact making positive changes to its role and sphere of influence. One of the primary ways we studied the problem was to ask a series of questions about whether security was more of a business enabler in the organization or more of a cost center.

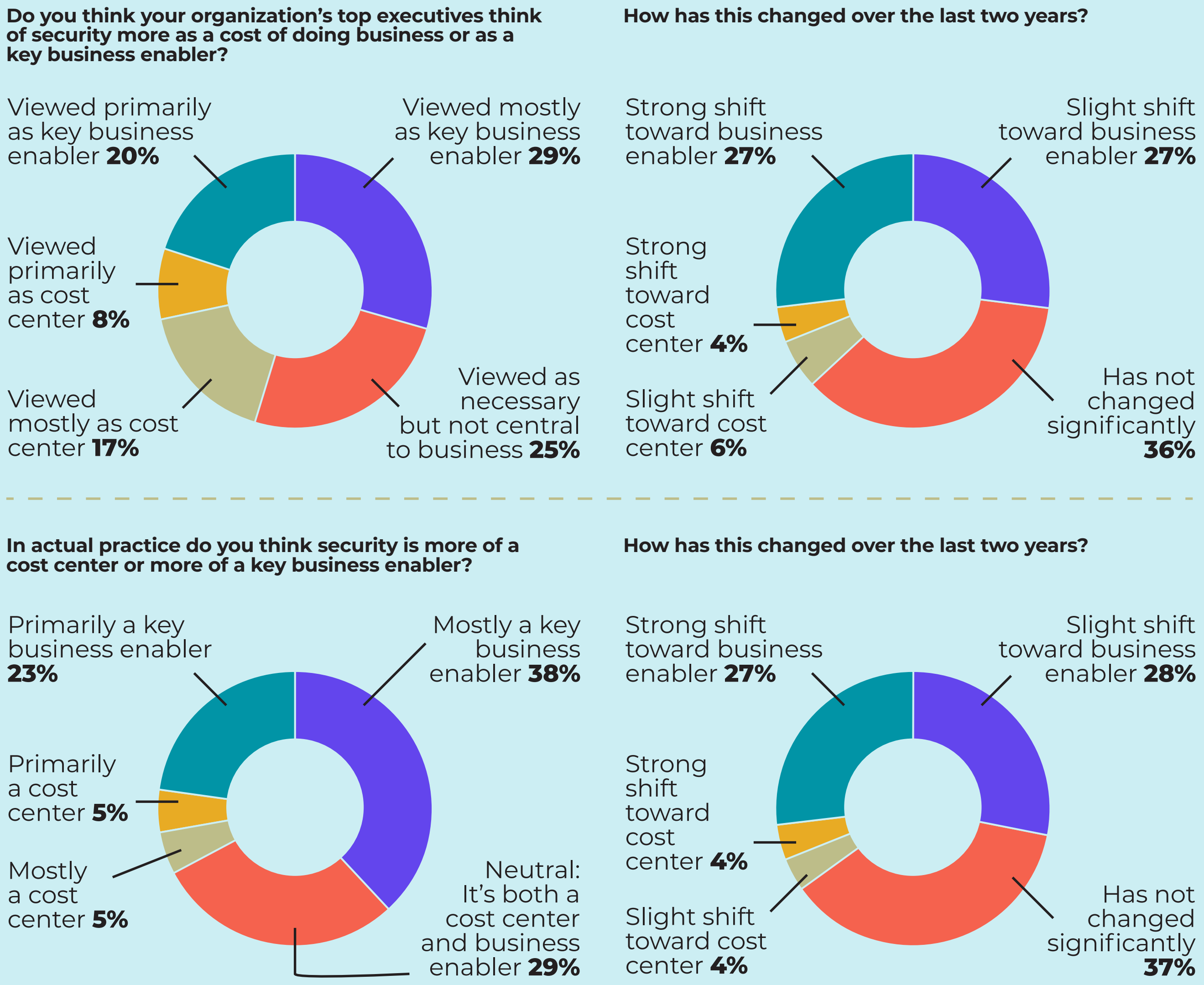
SECURITY AS BUSINESS ENABLER

The survey asked if top executives in the organization think of security as more as a cost of doing business or more as a key business enabler and how that had changed over the last two years. We followed by asking security professionals if they themselves thought security was more of a cost center or more of key business enabler, and how that perception had changed in the last two years. Results from all four questions point to security departments that have made positive shifts in organizational perceptions.

Half of security professionals said executives saw security as mostly or primarily an enabler of business goals, with 25 percent hedging, saying that executives saw security as both. One-quarter said security is mostly or primarily viewed as a cost center by executives (see Figure 2.1).

However, when looking at the trend over the past two years, security professionals see some shifts toward executives seeing security as busi-

Figure 2.1: Perceptions of Security's Role in Organizations



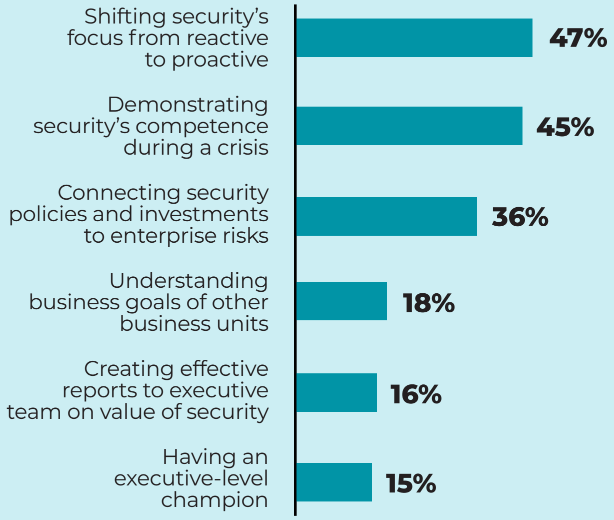
ness enablers. Just over a third—36 percent—said there had been no significant change, but those who said there was a shift toward a perception of security being a business enabler (54 percent) far outnumbered those saying there was a perception shift toward security being a cost center (10 percent).

Comparing what security professionals believe executives think to the actual ground truth of what they think is happening shows a small additional swing toward security serving as a business enabler for the organization. The question asked was, "In actual practice, do you think security is more of a cost center or more of a key business enabler?" Twenty-three percent said security was primarily a business enabler and another 38 percent said security was mostly a business enabler. Twenty-nine percent said security was both, and the final 10 percent said security was mostly or primarily a cost center.

Similarly, when security professionals were asked how this had changed in the last two years, 27 percent reported a strong shift toward business enabler and another 28 percent said there had been a slight shift. Thirty-seven percent said there was no significant change, while only eight percent said the pendulum had swung toward security operating more as a cost center.

The survey also asked what factors have the biggest impact on establishing security as business enabler rather than simply being a cost of doing business. Shifting security's focus from being reactive to being proactive topped the list with 47 percent of security professionals saying the factor was important. This was followed closely by "demonstrating security's competence during a crisis" at 45 percent, meaning the two choices are a statistical tie. The finding is interesting because the latter choice is taking advantage of security's reactive capacity to enhance its stature in the organization while the former expressly favors emphasizing proactive actions rather than reactive.

Figure 2.2: Factors Impacting Strategic Shift of Security



While the fact that diametrically opposing factors scored highest is interesting, it is not necessarily surprising and underscores a fundamental truth: No matter how strategic or proactive-oriented or business-enabler-minded a security department tries to be, it will always have a mission-critical role of responding to incidents. So when we talk about security becoming a business enabler or becoming more proactive, it is with the understanding that this is an expansion of security's role in ways that add value to the organization beyond the already valuable service of overseeing systems and processes that protect assets.

One of the primary ways security functions can use their expertise to add strategic value to the organization is by enhancing security's role in the organization's risk management process. In fact, 36 percent of security professionals selected "connecting security policies and investments to enterprise risks" as having one of the biggest impacts on establishing security as a business enabler—a finding bolstered by other results from the survey that will be discussed later. (See Figure 2.2 for complete results to the question of what factors were most important in supporting security's transition to being a business enabler.)

SECURITY AND RISK MANAGEMENT

The intersection of security and risk management continues to be a major topic for security professionals. Risk management is perhaps the clearest avenue for security to increase its strategic value in an organization. The importance of seeing security through the lens of risk has been growing as an idea for at least a couple of decades, and it is essential for any security leader trying to build a proactive security function to embrace security risk management.

In 2019, ASIS International published the Enterprise Security Risk Management (ESRM) Guideline as a largely aspirational document. The guideline is the reason this research used the term "business enabler" to study security's embrace of strategic roles in organizations. The concepts in the document remain largely aspirational today.

In the survey, nearly 6 in 10 security professionals report that security risk factors significantly in their organization's overall risk management approach—33 percent report striving to practice ESRM and another 26 percent said security risk was one of several risk factors when making risk-based decisions. Twenty-four percent said security risk practices were mostly or entirely influential only in making security decisions, and 17 percent said their security function did little or no security risk planning (see Figure 2.3).

We also wanted to see if there was a trend in the amount of time and resources devoted to security risk management. The results were not overwhelming but did point solidly in the direction of organizations working to increase security risk management capacity: 45 percent said they had devoted either somewhat more or significantly more time and resources in the last two years, 39 percent said it was mostly unchanged, while 16 percent said the time and resources devoted to security risk management had declined in the past two years.

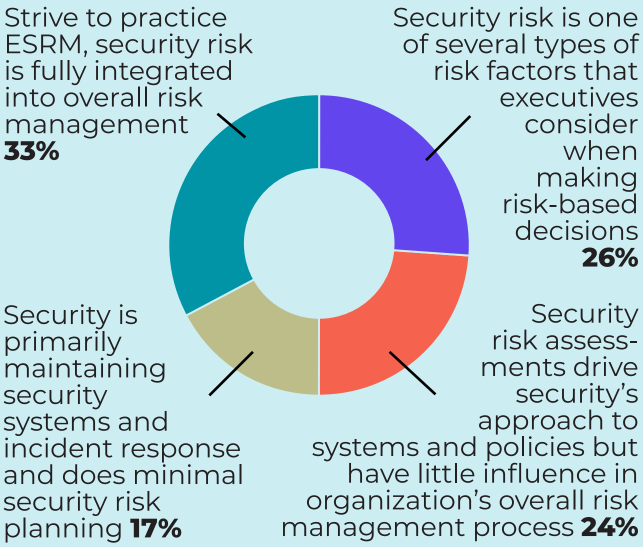
SECURITY BUDGETS AND OTHER FACTORS

A blunt way to examine organizational priorities is to look at budgets: organizations care about what they pay for.

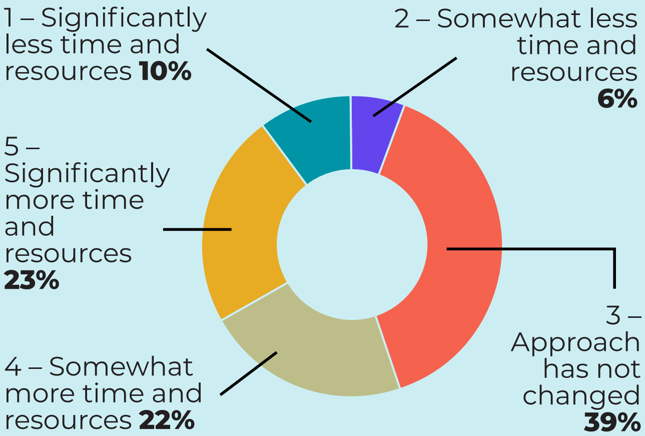
For comparative purposes, the survey asked security professionals first how they expected their organization's overall budget to change in the next 12 months, followed by asking them how they expected security budgets to change in the

Figure 2.3: Trends in Security Risk Management

Which best describes how your security department fits in with your organization's overall risk management function?



Rate if your investment of time and resources in security risk management is decreasing or increasing over the last two years.



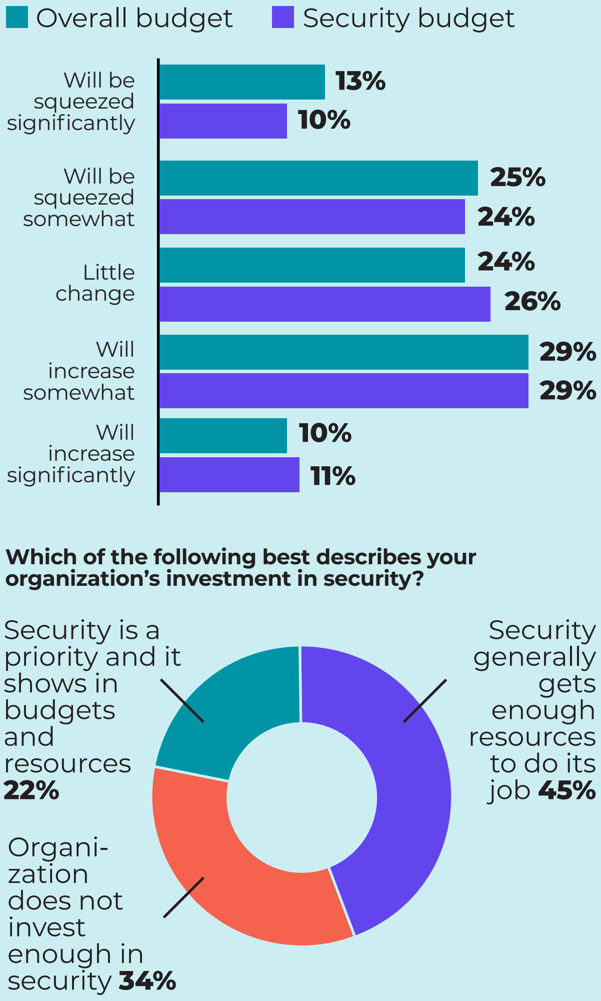
same timeframe. The results from both questions are remarkably similar, matching nearly identically and certainly falling within the statistical margin of error. In general, about a quarter expect no change in either, approximately 4 in 10 expect budgets to increase, and just less than that think budgets will decline (see Figure 2.4).

In addition, one-third of security professionals say their organization does not invest enough resources in security, leaving 45 percent who say security generally gets the resources it needs, and 22 percent who say that security is a priority in their organization, and it shows in budgets and resources allocated to it.

As part of the examination of security risk management, the survey asked security professionals to rate the importance of 10 different factors when making security risk assessments, giving the choices low importance, medium importance, and high importance. The 10 choices included selections specifically germane to security, such as the cost of lost, stolen or compromised assets, as well as more business-oriented factors, such as the potential negative impacts on profitability.

Figure 2.4: Budget Expectations

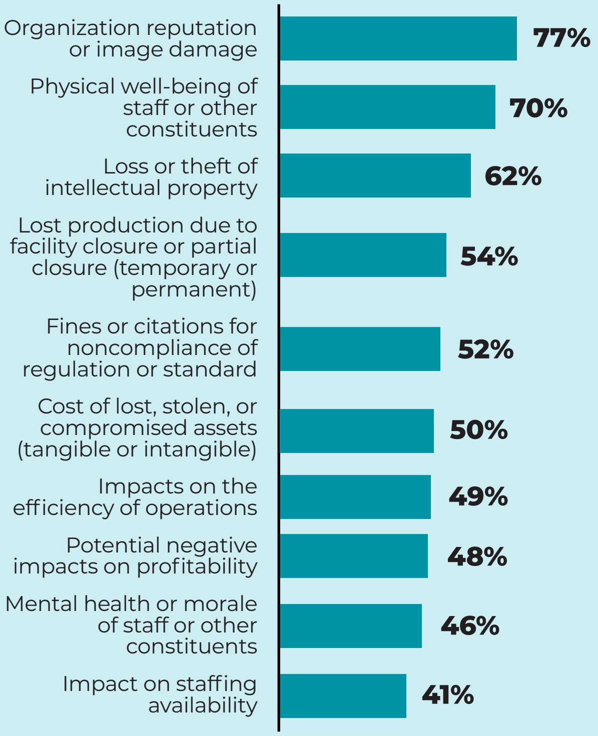
How do you think budgets will change in the next 12 months?



Which of the following best describes your organization's investment in security?

Figure 2.5: Important Factors in Security Risk Assessments

Percentage of security professionals who said the factor had a high importance.



Not surprisingly, only a few respondents rated any of the 10 factors as having a low importance. However, the factor that was rated highest was one of those business-oriented factors. "Organization reputation or image damage" scored highest with 77 percent of security professionals saying the factor had high importance in security risk assessments. The second highest was a more traditionally security-oriented factor: "physical well-being of staff or other constituents." At 70 percent, note that this is actually a statistical tie with reputation or image damage given the survey's margin of error of ± 4 percent (for full results, see Figure 2.5).

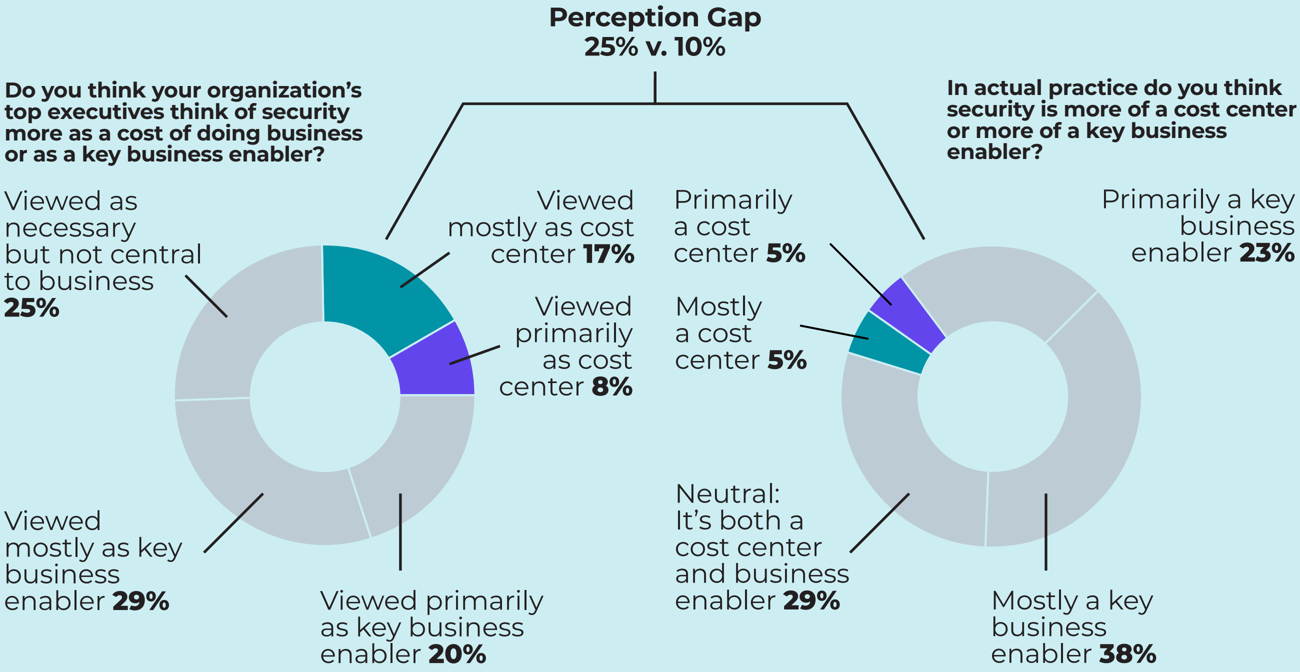
EVIDENCE SECURITY STILL HAS WORK TO DO

The previous section examined evidence showing security shedding its parochial image of rule givers and enforcers and growing into a valued strategic asset within organizations. This section will demonstrate that there are still gains to be made—in several cases using the exact same questions and outcomes.

Starting there and examining the second pie chart in Figure 2.3: While it may be encouraging that nearly half of organizations have increased investment in security risk management in the last two years, it leaves 55 percent of organizations that have not—including 16 percent that moved in the wrong direction. Likewise, the first pie chart of Figure 2.3 shows that more than 40 percent of security professionals report that security is not a factor in their organization's overall risk management function.

That presents a tremendous opportunity for security leaders to develop strategies and goals that reorient the department toward security risk and to incorporate security risk into the organization's other risk planning activities. We didn't ask the question, "Is it better for security to be reactive or proactive?" because—particularly when asking the question of security professionals—the outcome would be near unanimously "proactive." However, a major pathway for security to become more proactive is to maximize its emphasis on security risk management while

Figure 3.1: The Gap in Perceptions of Security's Role in Organizations



working to incorporate security risk more widely in the organization.

Similarly, Figure 2.1 depicts the perceived attitudes security professionals have of their organization's leaders as well as their own perceptions of how much security acts as a business enabler compared to being thought of as the cost of doing business. Both sets of findings bolster the finding that security has become more strategic than it used to be, and that it is trending in the right direction. However, there is a small but noticeable gap between the two sets of perceptions. Ten percent of security professionals said that in actual practice, security is mostly or primarily a cost center. However, 25 percent said the organization's top executives thought of security as mostly or primarily a cost center. That's a perception gap that security professionals need to continue to find ways to address (see Figure 3.1).

Another sign that security has work to do comes from a question dealing with budgets and acquiring resources. Figure 2.4 presented evidence that security had made headway in these areas. However, the survey also asked, "Compared to other departments, is it harder or easier for security to get approval for projects or additional assets?" More than half (55 percent) reported that other departments in general had a much easier or somewhat easier time to get approval for projects and resources (see Figure 3.2).

Finally, the survey asked security professionals if they calculated security's return on investment (ROI) for the organization. It's another one of those good sign/bad sign results: 53 percent said they did and 47 percent said they did not (see Figure 3.3). Years ago, very few security departments would be concerned with concepts like ROI. The research shows approximately half do

Figure 3.2: Security Has More Trouble Getting Needed Resources

Compared to other departments, is it harder or easier for security to get approval for projects or additional assets?

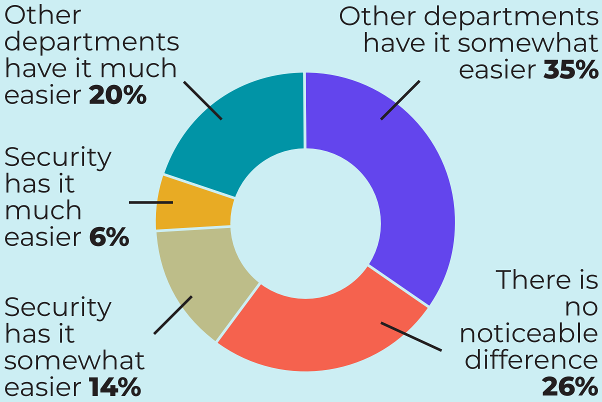
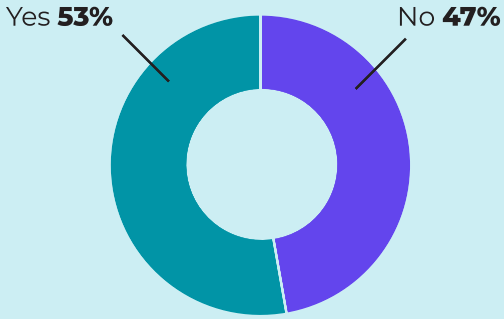
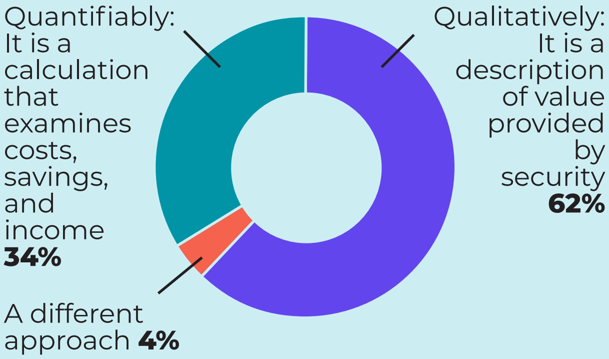


Figure 3.3: Security ROI

Does your organization evaluate the return on investment of security spending?



Which of the following best describes how your organization approaches security ROI?



so now, which, when considering the difficulties of measuring security ROI versus, say, marketing ROI, is worthy of note.

ROI as a concept is a financial measure designed to assess the monetary value of the subject being studied. Underscoring the difficulty of doing this in relation to security, only one-third of those who said they evaluate security ROI do so quantifiably, leaving 62 percent who use qualitative measures, and four percent who use both or some other way to present ROI.

The themes presented in sections two and three of this report are all interrelated and, admittedly, incomplete. Security brings value to an organization when it is a major contributor to establishing an environment in which the organization can thrive. Getting there, however, has required an evolution in how security professionals think about security and the way they present security to the rest of the organization. This evolution has been underway for years now, and this research provides clear evidence that security has found success in changing the stature and importance of security in organizations, while showing at the same time that there is more room for growth.

Working to make security an important part of an organization's approach to risk management is one enabling factor, so is being able to communicate with executives in terms that matter to their understanding of the business—such as return on investment. These are merely part of a bigger picture that is described very well in the ASIS ESRM Guideline. For security to thrive, and more specifically for security to help organizations thrive, they must create partnerships with other organizational functions that fuel mutual respect and mutual success.

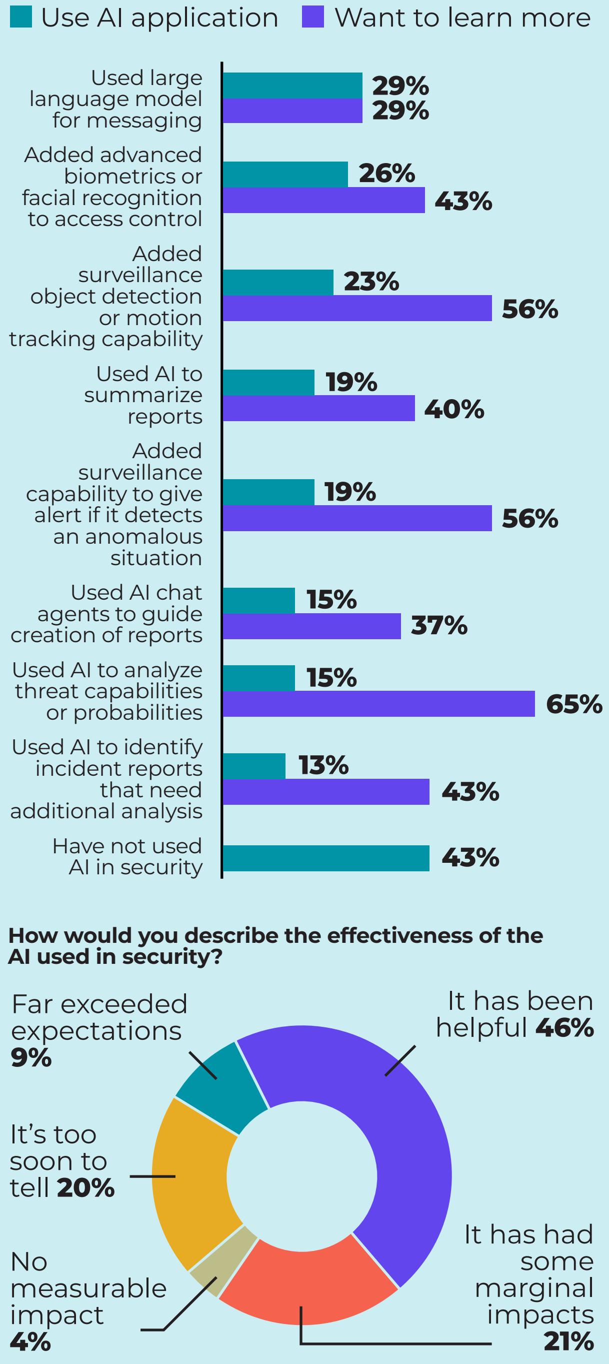
SECURITY'S KNOWLEDGE AND USE OF ARTIFICIAL INTELLIGENCE

Much of this research studied trends focused on security's role and stature in the organization. However, no 2025 trends analysis can ignore artificial intelligence (AI), the rapidly expanding technological advancement that has begun to revolutionize how organizations use technology to help achieve goals. Security may not be on the absolute bleeding edge of AI, but security's use of AI is more advanced than many other functions. One of the primary reasons for this is that security systems—namely surveillance camera systems and physical and logical access control and monitoring systems—produce vast amounts of data. More data, in fact, than could ever be monitored and analyzed by human security teams. Analyzing mountains of data to achieve actionable outcomes is exactly the scenario in which current AI applications excel.

As a result, the research shows that use of AI is high among security professionals—57 percent report their organization uses AI in some capacity in security—and interest is even higher. Using a large language model (such as Chat GPT) to craft messaging tops the list (29 percent), followed by incorporating advanced biometric screening, such as facial recognition (26 percent), and incorporating AI into surveillance for object detection or motion tracking (23 percent). See Figure 4.1 for a breakdown of different ways AI is used in security.

Despite the embrace of AI, no single use of AI has particularly high adoption rates (see green bars in Figure 4.1), however, interest in learning more about capabilities is high (see purple bars in Figure 4.1). These results signify that security

Figure 4.1: How Security Uses AI



How has your organization's security function made use of AI or machine learning and what are you interested in learning more about?

How would you describe the effectiveness of the AI used in security?

Note: Asked of those who report using AI in some way.

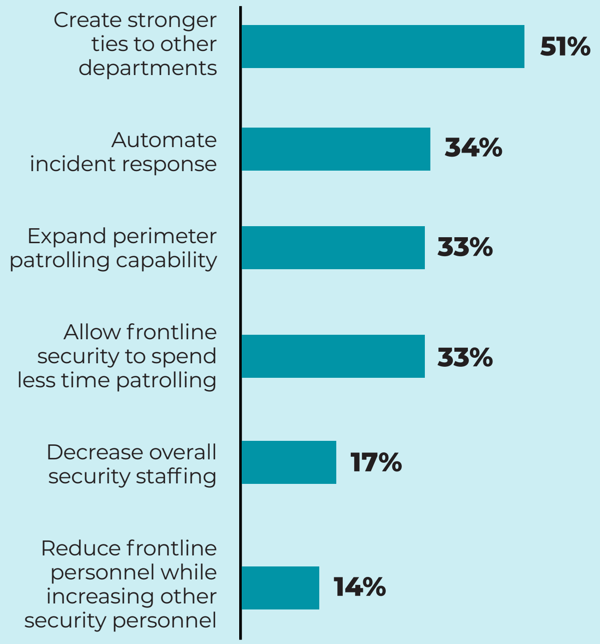
—like other functions—still has opportunity and interest in utilizing AI to increase security's effectiveness.

Of those who reported they use AI in some way in security, there is general positivity about its effectiveness: 46 percent say it has been helpful and 9 percent say it has far exceeded expectations. One-in-five security professionals (21 percent) report that AI has had some marginal security impact, and only 4 percent say it has had no measurable impact. That leaves 20 percent who said it was too early to tell if AI was having a positive impact.

Security's use of AI dovetails nicely with the previous sections of this report when examining the benefits of security AI usage. Topping the list—among security professionals who reported that their organizations used AI in security in some way—51 percent said using AI helped them create stronger ties to other departments through information sharing or collaborative technology projects (see Figure 4.2).

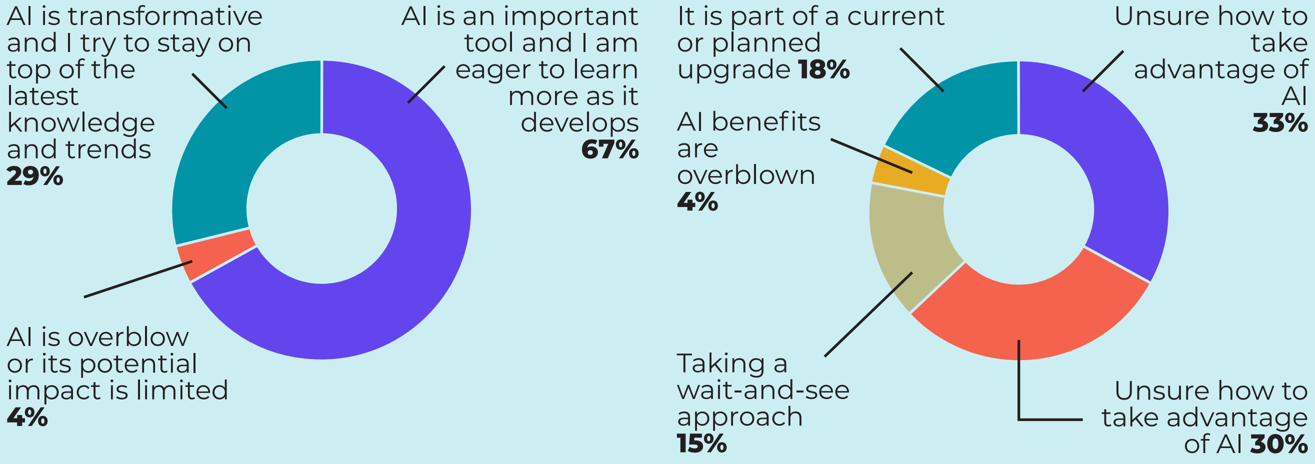
Figure 4.2: Security Changes as a Result of AI

Has AI enabled you to do any of the following?



Note: Asked of those who report using AI in some way.

Figure 4.3: Impressions of AI in Security


What best describes your knowledge and level of interest in how AI can or will improve security?

Why has AI not been used in security?

Other reported benefits: automated incident response (34 percent), expansion of perimeter patrol capability (33 percent), and shifting the role of frontline security away from patrolling and toward investigation, response, and management (33 percent). Fewer security professionals report that AI led to a decrease in overall security staffing (17 percent) or a decrease in frontline security personnel and subsequent increase in other security personnel (14 percent).

Among security professionals reporting they have not used AI in security, it is not because they think AI lacks potential: only 4 percent said "AI benefits were overblown." The two most typical reasons why AI was not being used in security is that security professionals are unsure how to best take advantage of AI in security (33 percent) and that security has limited resources and needed to prioritize other areas (30 percent). Eighteen percent said AI was part of a current or planned upgrade, and 15 percent reported they were taking a wait-and-see approach. Overall, 96 percent of all security professionals in the survey said AI is either an important tool or a transformative tool (see Figure 4.3).

WHY THESE SECURITY TRENDS MATTER

Up to now, we have presented findings with an implicit assumption that when security is engaged at a strategic level in the organization it leads to more successful security outcomes. The survey also asked several questions that help to understand if organizations are in fact experiencing those positive security results. In one question, we listed 12 security outcomes and asked security professionals to assess if those outcomes had improved or worsened in the previous year based on a five-point scale. As expected, the results skew toward the better side of the scale. However, putting those who answered "somewhat better" or "significantly better" into one group and those who answered "significantly worse," "somewhat worse," and "little or no change" into another group yielded results that could then be used for comparison.

Figure 5.1 is a table showing the baseline results to these questions as well as an overarching question that also used the same five-point scale, in which we asked, "Overall, has your organization's ability to protect its assets improved in the last two years?" Note that the table shows the combined grouping percentages as well as a weighted average where higher numbers represent more answers on the better side of the

Figure 5.1: Baseline for Effectiveness Measures

In the past year or so, have the following security-related areas and issues improved or gotten worse at your organization?

	Same or worse	Better	Weighted average
Ability to anticipate and prepare for adverse events	38%	62%	3.78
Ability to investigate incidents	36%	64%	3.83
Capability to identify and deal with insider threats before they become a problem	49%	51%	3.64
Ability to fill security vacancies with qualified people	62%	38%	3.15
Frequency of and support for security training and drills	51%	49%	3.51
Common access control breaches, such as propped doors, tailgating, or piggybacking	52%	48%	3.51
Effectiveness of surveillance technology	38%	62%	3.78
Process of identifying threats and completing risk assessments	41%	59%	3.73
Stature of security as an important department within the organization	40%	60%	3.72
Ability to mobilize in an emergency	38%	62%	3.81
Collaboration with external security partners, such as law enforcement	38%	62%	3.83
Opportunities to engage senior executives or board on security issues	41%	59%	3.71
Organization's ability to protect its assets*	37%	63%	3.73

*This question was asked slightly differently. It asked if the ability had improved in the last two years.

scale. Weighted averages are useful in making statistical comparisons. The complete data for the questions is presented here for benchmarking purposes. To gauge the impact of security trends, we used the parts of this question most germane to overall security effectiveness or to the specific trend being studied.

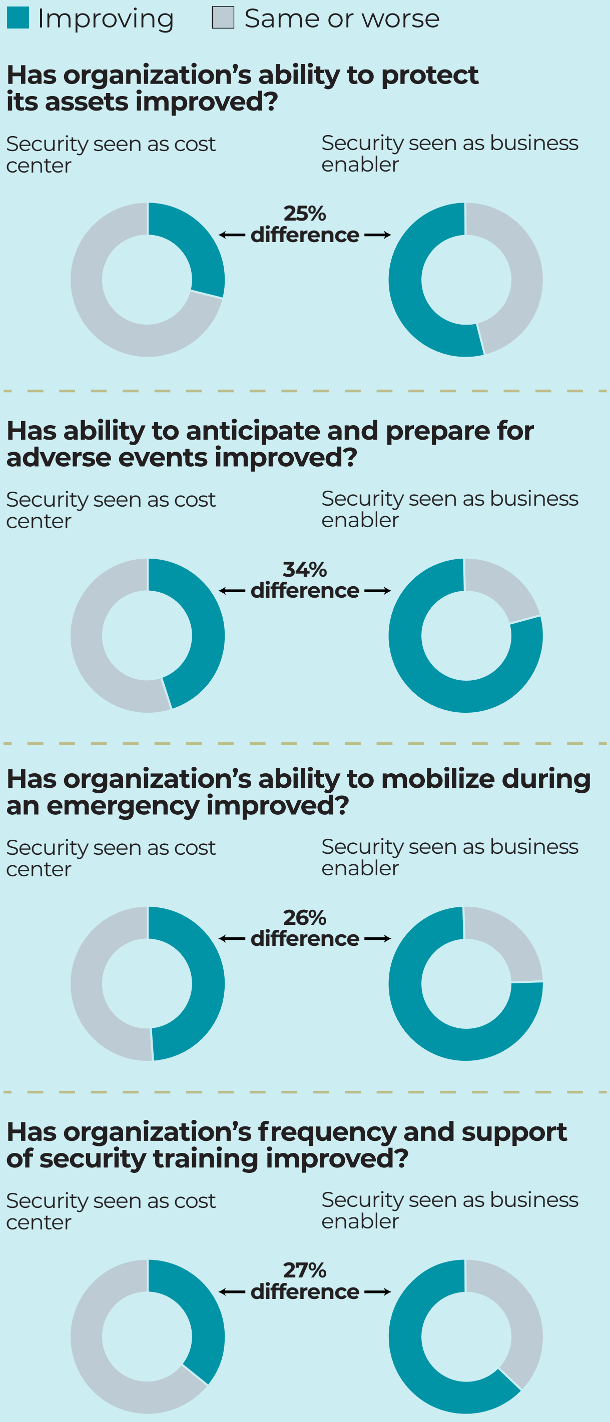
IMPACT OF SECURITY BEING A BUSINESS ENABLER RATHER THAN COST CENTER

Recall from section two of this report that security professionals were evenly split on whether executives viewed security as a business enabler (49 percent) or as a cost center (50 percent when combined with not central to business). Likewise, security professionals were split when it came to their own perceptions of how security fit in the organization, with 61 percent saying security was a business enabler and 39 percent saying it was a cost center (when combined with those who said it was both).

These relatively even splits provide useful segments for comparison when examining the effectiveness measures outlined above. At organizations where executives view security as more enabler than cost center, 54 percent of security professionals said the organization's ability to protect its assets had either somewhat improved or significantly improved. This is a 25 percent gap compared to those who saw improvement at organizations where executives view security as more of a cost center (29 percent).

As Figure 5.2 shows, the difference persists when looking at more granular outcomes. For example, 79 percent of the security professionals who say their executives see security as a business enable say that their organization's ability to anticipate and prepare for adverse events has improved compared to last year. This compares to 45 percent of those who work at organizations

Figure 5.2: Security Impact of Having Executives Who Think of Security as a Business Enabler



where executives see security as more of a cost center, meaning there was a 34 percent gap between the two. The survey yielded similar results when examining the ability to mobilize during an emergency (26 percent gap) and frequency and support of security training (27 percent gap).

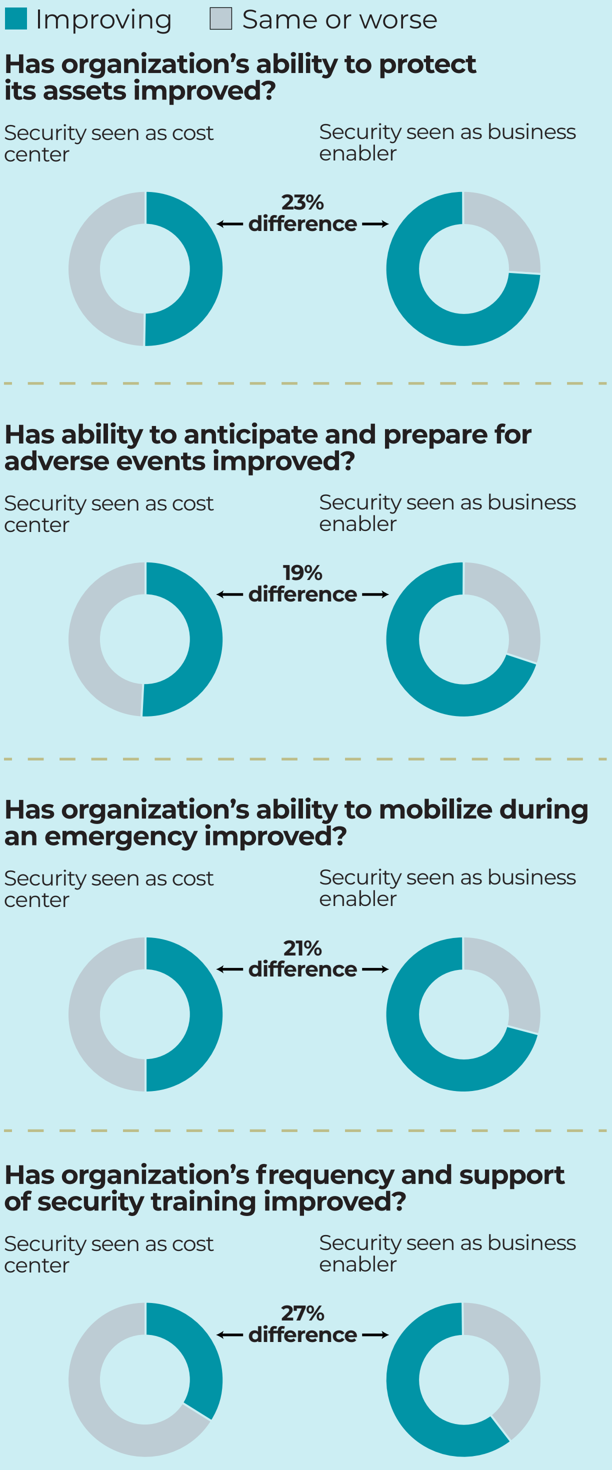
Also recall from section two that 55 percent of security professionals thought there had been a strong or slight shift toward the security function serving as a business enabler in their organizations, leaving 45 percent who said there had not been change or there had been shift toward security being a cost center. This close split provides another opportunity to study effectiveness.

Just as in the previous example, there are strong correlations between security shifting toward being a business enabler and the effectiveness of the security function. Almost three-quarters (74 percent) of those who said there had been a shift toward business enabling reported that the organization's ability to protect its assets had improved in the last two years. That compares to 51 percent among security professionals who said the security's scope had not changed or had shifted to being more of a cost center, yielding a difference of 24 percent (see Figure 5.3).

The difference for anticipating and preparing for adverse events was a little less at 19 percent (70 percent of those in organizations shifting toward business enabling, 51 percent in the rest). The difference when comparing the effectiveness of mobilizing during an emergency was 21 percent (71 percent to 49 percent) and for the frequency and support of security training, the difference was 27 percent (61 percent to 34 percent).

The ratios change some, but the same trend holds when comparing these effectiveness measures to security professionals who say their ex-

Figure 5.3: Impact of Security Being More of a Business Enabler in Practice



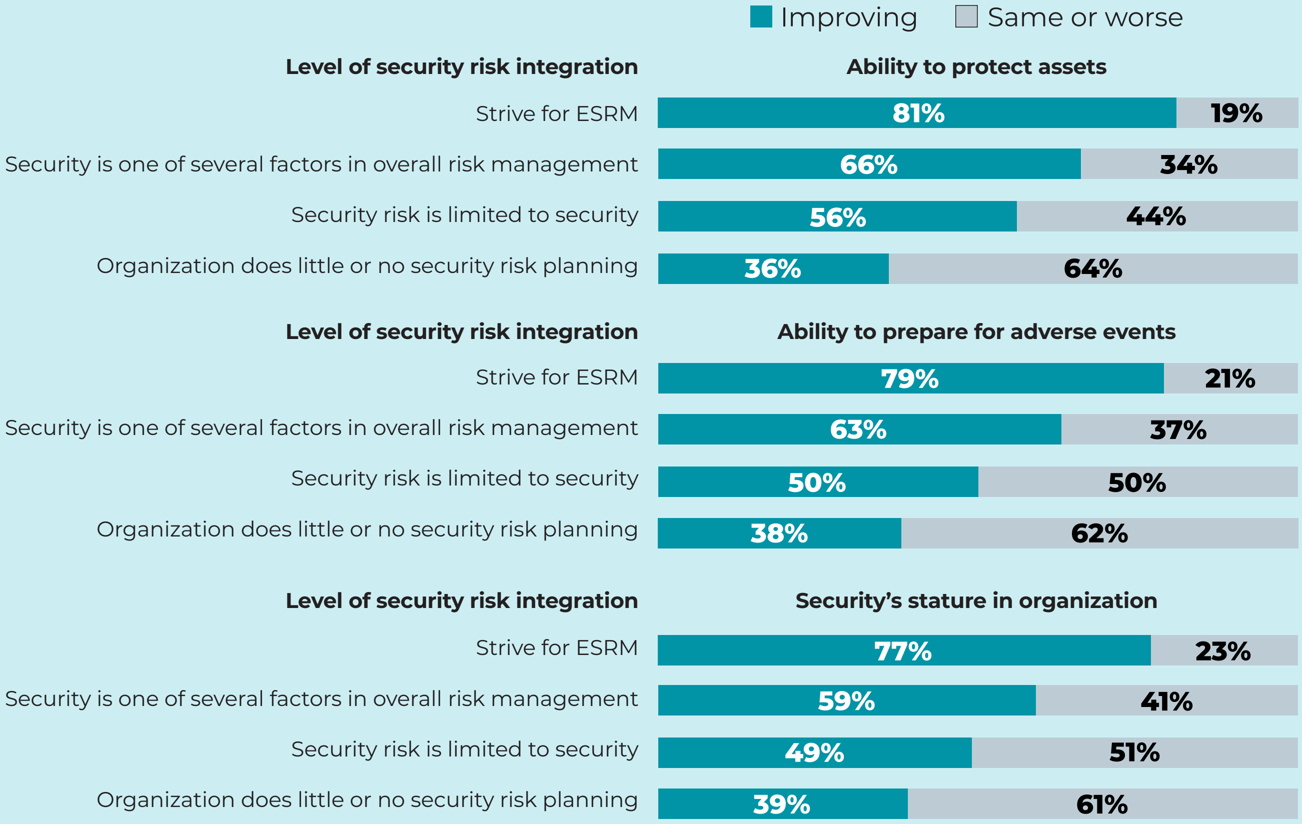
ecutives are trending toward seeing security as a business enabler versus a cost center. The data is less clear when considering security professionals' perceptions of where the security function falls on the business enabling versus cost center comparison. More than 60 percent of security professionals were on the business enabler side, and when looking at these effectiveness measures, the differences are much smaller than the other comparisons presented here.

IMPACT OF SECURITY BEING PART OF ORGANIZATION'S RISK MANAGEMENT PROCESS

Figure 2.3 presented the findings of how important the security department is to the organization's overall risk management function. The question asked security professionals to select the best description of security's risk integration level, giving four choices that got progressively more integrated:

- Security is primarily maintaining security systems and incident response and does minimal security risk planning (17 percent).
- Security risk assessments drive security's approach to systems and policies but have little influence in organization's overall risk management process (24 percent).
- Security risk is one of several types of risk factors that executives consider when making risk-based decisions (26 percent).

Figure 5.4: Impact of Security Risk Management



- Organization strives to practice ESRM, security risk is fully integrated into overall risk management (33 percent).

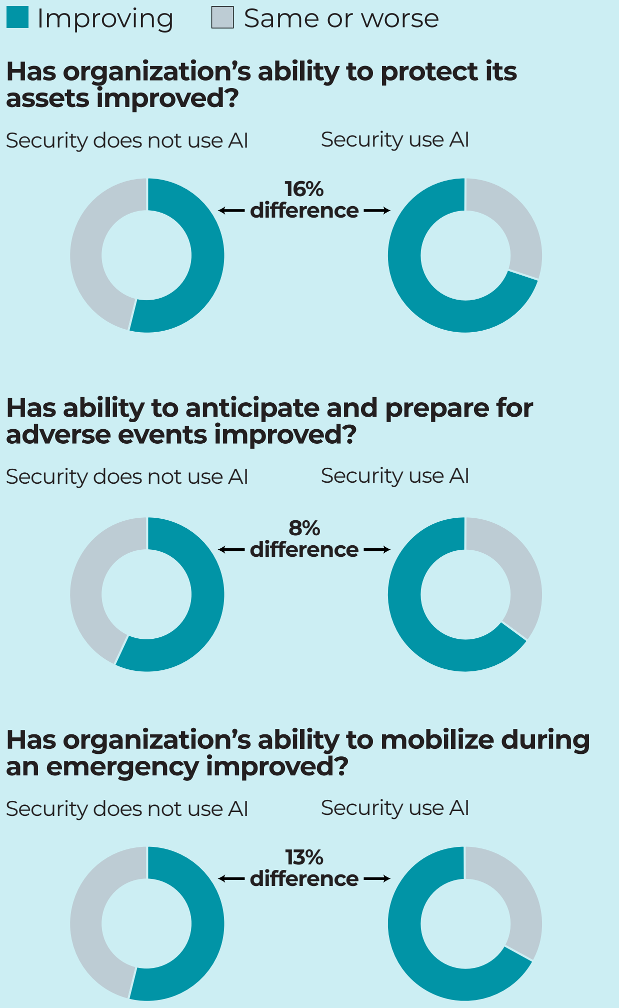
Figure 5.3 shows that the more integrated security is in the organization's overall risk management, the more effective security is at the organization. Using the same five-point scale groupings as previously—somewhat or significantly improved as one group and the same or worse as the other—for each measure, the number of security professionals who said the measure improves grows as the amount of risk integration increases.

When examining the organization's ability to protect its assets, 81 percent of security professionals who said their organizations strive for ESRM also said the organization's ability to protect assets was improving. That falls to 66 percent for security professionals at organizations where security is one of several risk factors considered in risk management. It decreases again, to 56 percent, when security risk management is mostly contained within the security department, and it plummets to 36 percent at organizations that do minimal security risk management.

The same patterns emerge when examining other effectiveness measures. Notably, 80 percent of the ESRM group say the ability to anticipate and prepare for adverse events has improved in the last year. That falls to 50 percent when security risk management is kept within security and to 38 percent at organizations that do little risk management.

HOW AI USE AFFECTS SECURITY EFFECTIVENESS

Figure 5.5: Impact of AI on Security's Effectiveness



There is evidence that using AI increases security's effectiveness using these measures, though the evidence is weaker than the other factors in this section. This is not surprising; for one, the study took a broad interpretation of what constituted using AI in security, including simply using large language models in crafting messaging. Such limited use could hardly be expected to make significant impacts on security outcomes. Not enough security professionals reported using some of the more advanced AI tools the survey asked about to be able to do meaningful effectiveness calculations.

Despite the trends not being as strong, they are there. Likely fueled by those using more advanced AI applications, 70 percent of those using AI say the organization's ability to protect its assets is improving. This compares to 54 percent of security professionals who report they have not used AI in security (see FIgure 5.5).

Likewise, we see the same trends as in the other comparisons, but with smaller differences. Of those using AI, 65 percent say their ability to anticipate and prepare for adverse events has improved, compared to 57 percent of those who have not used AI. Looking at being able to mobilize during an emergency, 67 percent of those using AI say it is improving, compared to 54 percent from organizations not using AI in security.

METHODOLOGY

This research project commenced in October 2024 when ASIS International Content Development Director Scott Briscoe reached out to several ASIS members to convene the project's volunteer group, including representation from the project sponsor, Resolver. The volunteer group shaped the survey questionnaire, which was deployed in November and December 2024. Security consultants and representatives from business partners who have products or services for the security profession were given the option of answering the same questions as security professionals based on their knowledge and experience or answering an alternate set of 10 questions. Results from the consultants part of the survey were not covered in this report and will be presented in a future article in ASIS's magazine, *Security Management*.

Overall, a total of 728 people answered at least some of the questions, and 539 completed the last question available to them. Data presented includes all data for that question, whether or not the survey was completed. This response yields a margin of error of ±4 percent at the 95 percent confidence level for most of the questions and ±5 percent at the 95 percent confidence level for some of the calculations.

The following table presents demographic information of the participants. The results are consistent with other studies conducted by ASIS and are similar to demographics of ASIS members. *Unlike previous surveys, participants were given the option to choose multiple regions.

Facility Scope	
Multinational with a variety of facility types in multiple countries	26%
Variety of facility types in multiple regions or locations, primarily within single country	32%
Multiple facilities primarily in a single region	26%
Mostly a single facility or single campus with a few facilities	15%

Region*	
North America	47%
Central America, South America, Caribbean	15%
Europe	17%
Middle East	14%
Africa	24%
Oceania	6%
Asia	24%

Number of Employees (or Employees and Students)	
1 to 100	18%
101 to 1,000	21%
1,001 to 10,000	28%
10,001 to 50,000	17%
50,001 to 100,000	7%
More than 100,000	9%

Industry	
Amusement, gambling, or recreation	1%
Banking, finance, insurance	9%
Consulting and professional services	3%
Defense and intelligence	6%
Education, K-12	2%
Education, university	3%
Emergency Services	1%
Food and agriculture	2%
Healthcare	5%
Hospitality and food services	2%
IT and telecommunications	5%
Law enforcement	3%
Manufacturing	10%
Media and entertainment	2%

Museums and cultural properties	2%
Oil, gas, chemical	7%
Pharmaceutical	2%
Public administration/government (nondefense, law enforcement, or education)	4%
Real estate and construction	1%
Retail	3%
Security services	17%
Transportation and supply chain	4%
Utilities	2%

Title	
Senior executive (usually chief or VP)	14%
Report to senior executive	37%
Mid-level management	31%
Low level management	9%
Frontline or administrative	9%