ASIS INTERNATIONAL | SECURITY ISSUES RESEARCH

THE CURRENT STATE OF SECURITY RISK MANAGEMENT

BENCHMARKS AND EFFECTIVENESS MEASURES

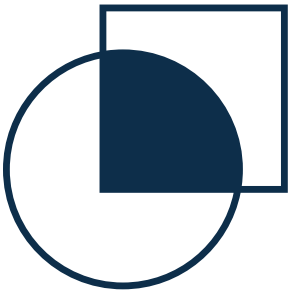
Sponsored by LifeRaft

CONTENTS

SUMMARY

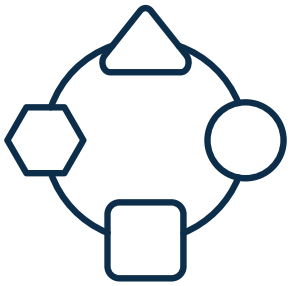
ASIS International continued its Security Issues Research program with a project on security risk management. The financial and content contributions from our partner and sponsor LifeRaft made the project possible.

A small group of ASIS volunteers established the themes and helped put together a survey instrument that ultimately more than 1,000 security professionals and others answered. ASIS staff led conversations on the topic with a dozen members to help understand and add context to the survey findings. The results provide excellent opportunities for benchmarking security practices as well as ideas on the types of critical success factors that can help security professionals build the most successful security risk management practice possible. Key findings from the report include the following.



1. SECURITY PROFESSIONALS FACE A COMPLEX AND OVERLAPPING SECURITY THREAT LANDSCAPE.

Threat assessment is a key component of any security risk management process. The research shows that organizations face an incredibly diverse set of threats. New threats continuously emerge, but rather than replacing older threats, the new layers on top of the old. Security professionals are generally dealing with multiple threats and incidents at one time, creating the dynamic one expert described as being in “permacrisis.”



2. SECURITY PROFESSIONALS USE A VARIETY OF METHODS TO IDENTIFY THE SECURITY THREATS THEIR ORGANIZATIONS FACE.

The survey presented several different methods security professionals could employ to identify threats and asked them to rank how important they are. While internal threat assessment teams scored highest, perhaps the more interesting finding is that every method scored extremely highly. The finding underscores both the importance for security professionals to seek diverse inputs when working to identify threats as well as the important role threat identification has in security risk management planning.

3. SECURITY LEADERS OFTEN LACK THE ORGANIZATIONAL STATURE TO DRIVE STRATEGIC RISK MANAGEMENT DECISIONS.

Confirming a finding from previous ASIS Foundation research, security—in both perception and practice—is more focused on tactical initiatives than strategic outcomes. Security leaders who have significant impact in their organizations’ strategy say the main reason they achieved that impact was having the support of the CEO. Among the tactics used to try to build more influence, two lead the way: building rapport with other business units and capitalizing on security’s important role during times of emergency or crisis.

4. SECURITY RISK MANAGEMENT PLANS ARE HIGHLY EFFECTIVE

When the threats turn into actual incidents, security professionals report that most of the time their security risk management plan both had identified the threat and helped the organization mitigate negative consequences.

5. THE RESEARCH IDENTIFIED FOUR CRITICAL SUCCESS FACTORS FOR EFFECTIVE SECURITY RISK MANAGEMENT

- Using and regularly updating a security risk management plan
- Security leaders who spend 50 percent or more of their time on strategic rather than tactical issues
- Security having an important role in the organization's overall risk management process
- Implementing enterprise security risk management

Each of these factors either led to fewer critical incidents for which organizations were unprepared or led to a rating of having a highly effective overall risk management strategy as an organization or both.

6. ESRM HAS EMERGED AS A KEY DIFFERENTIATOR

While questions related directly to ESRM were limited, the research showed that ESRM is widely embraced and, as mentioned, when security leaders are actively working to implement ESRM it leads to better risk management outcomes than organizations where ESRM is not a priority.

INTRODUCTION

At its most basic level, corporate security is protecting assets—there's a reason the seminal work in the security field is called, *Protection of Assets*. However, how assets get protected has evolved significantly over the last 20 or 30 years. Where corporate security could at one time function well while primarily being a reactionary discipline, it evolved into one that requires a proactive, strategic approach to protecting assets.

Being proactive about the protection of assets means knowing what assets your organization has, understanding what threats could compromise those assets, and developing appropriate processes and strategies to negate or minimize the impact of the threats. Most organizations understand that this proactive approach to the protection of assets is security risk management.

To be clear, this evolution has been far from a straight and easy path to follow. For one thing, it's not like corporate security could flip a switch and no longer need to be reactionary. In fact, being reactionary is still a major security responsibility: If an alarm sounds or an incident occurs, security must answer the call. Everyone understands the reactionary parts of protecting an organization's assets, which fall under incident or emergency management processes.

Gaining the authority and the organizational standing to be proactive in protecting assets, is another matter. And so ASIS International undertook this study to get a glimpse of the current state of security risk management, to understand how far security has shifted toward a desired proactive state; what factors contribute to progress and what obstacles security leaders face; and what characteristics make corporate risk security management effective.

To begin to examine those issues, we start by trying to understand the threats organizations face and how they affect security risk management.

Acknowledgment

ASIS would like to thank the following volunteers for their valuable contributions to this project:

Gigi Agassini, CPP
Security Consultant

Mark Ashford
Corporate Security, Policy & Relations
Central Bank of Ireland

Diana Concannon, PCI
Associate Provost, Strategic Initiatives and Partnerships
Dean, California School of Forensic Studies
Alliant International University

Rhys Robinson
Senior Client Success Manager
LifeRaft

Scott Wolford, CPP
Security Manager, Grandview Yard
Nationwide Mutual Insurance Company

Matt Jones
Assistant Director, Capitol Security & Visitor Services
Washington State Department of Enterprise

SEEING AND IDENTIFYING THREATS

The survey provided 12 common security threats an organization might face and asked participants to choose the ones that presented the biggest risks to their organizations—they could choose up to three. While there is clear separation between the top of the list and the bottom (see Figure 1.1), the first thing to notice is how distributed the responses were. All of them were selected as a top concern by a good number of security professionals, and eight of 12 were selected by more than a quarter of participants.

Failures in any of the threat areas could prove extremely costly for any organization, however it is not surprising that "workplace violence or active assailant" (43 percent) and "ransomware or other cyberattacks" (42 percent) were at the top of the list. Almost all of the survey participants have some relationship to physical security, with security professionals being the primary target of the research. In addition, 47 percent of respondents who listed a location were from North America, where workplace violence, which includes the alarming trend of increasing mass casualty incidents, has topped the list of security professional concerns for a decade or more. Similarly, the fact that so many vital systems are connected by computer networks and have highly complex vulnerabilities means the IT systems are both difficult to protect and attacks can be crippling to an organization—and the high-profile incidents in both categories make the news.

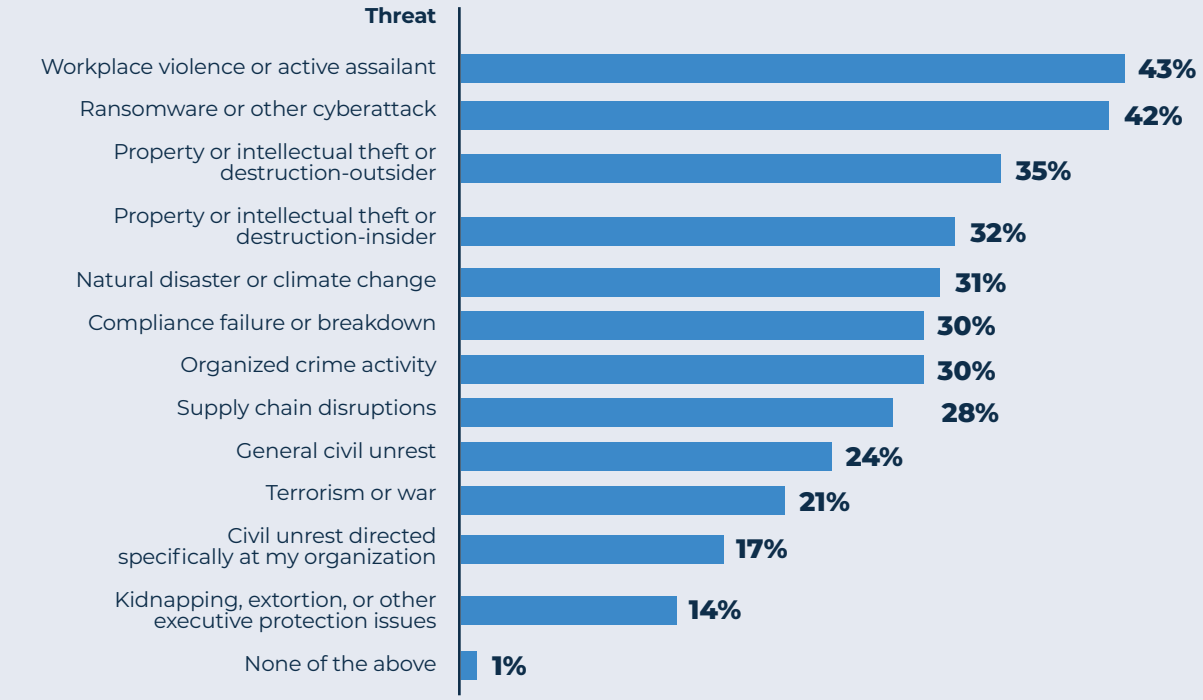
Looking down the list of threats, "kidnapping, extortion, or other executive protection issues" was selected by the fewest number of security professionals, yet it was still chosen as one of three primary threats by 14 percent of them.

Diana Concannon, a long-time ASIS volunteer, security consultant, and dean of the California School of Forensic Studies at Alliant International, pointed out that the threats do not happen in isolation. The threats become interrelated, and as incidents in one area occur, they affect new incidents that occur in a different area. It leads to what she described as a permanent state of crisis, or "permacrisis" for security leaders.

Michael Gips, CPP, principal at Global Insights in Professional Security, said the confluence of physical security risks and cybersecurity risks is what has made security risk management so complex. He recounted the journey security has taken starting at a time when physical security procedures were central and information security was an afterthought. He mentioned milestone events, how the security function after 9/11 increased in importance, particularly focused on terrorism and extremism. While that never receded as an issue, the urgency did wane over the decades. We then entered a time when computer network vulnerabilities began to usurp security attention. Social media rose and the prospect and danger of insider threats led to entire security teams dedicated to mitigating insider threats.

"Now you have cyber-physical combination issues, social media, disinformation campaigns—you have to worry about brand reputation," he said. "Everything is enabled by and attached to networks and technology, all of which can be highly vulnerable. And now there's AI, what will that mean for us? I know this is like a 30-year trip through security history, but the point is, the old saying 'There's nothing new under the sun' is wrong. Security is constantly facing new threat vectors, and the old ones are still there. They don't go away. The new threats layer on top of the old, and it keeps getting more and more complex."

Figure 1.1: Threats that Pose the Most Risk to an Organization



For each of the threats the survey asked security professionals if they had experienced any incidents that had a significant impact on their operations, profitability, or reputation (Note: property or intellectual theft was combined into a single category for that question). Three-quarters said that they had. In fact, more than half (52 percent) had experienced incidents in more than one category, and 18 percent had experienced incidents in four or more of the categories (see Figure 1.2).

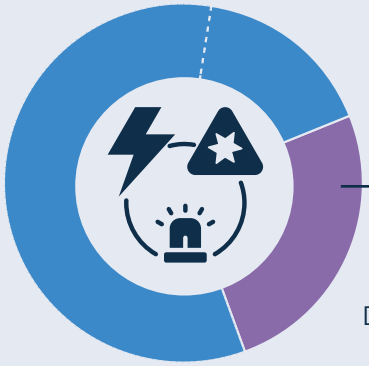
Now that we know the types of threats that pose risks to organizations, what methods do security professionals use to identify the threats? The survey asked participants to rate the importance of six different threat identification methods using a five-point scale, with a rating of one being "minimal importance" and a rating of five being "critically important." Not surprisingly, all six methods in the study skewed strongly to the critically important side of the scale (see Figure 1.3). The method rated least important—gathering "information from subject matter experts, such as in webinars, articles, or conference sessions"—still had a weighted average of 3.89, with two-thirds of respondents rating it either a four or five.

The top-rated method was using "internal threat assessment and intelligence teams," which garnered a weighted average of 4.42 and a whopping 62 percent who rated it a five, or "critically important." Another interesting finding: Participants were offered the choice to say they did not use any of the researched methods. Showing just how important threat identification is, every method was used by nearly every survey participant.

"I've been on a bunch of working groups to come up with risk assessment guidelines and risk

Figure 1.2: Experienced an Incident that Caused Significant Impact

75% Experienced at least one type of significant incident (**18%** experienced four or more types of incidents)



25% Did not experience a significant incident

25% experienced a natural disaster or climate change

23% experienced a compliance failure or breakdown

23% experienced a supply chain disruption

21% experienced general civil unrest

20% experienced organized crime activity

management guidelines for all these groups, and they're all the same," said Caroline Ramsey-Hamilton, CEO of Risk and Security LLC, in a focus group. "It includes having a threat analysis. You have to go and see how likely the threats are to occur first in your geographic area, but also in your industry. How often have they happened in the past? And then you have to look at the control. I have a set of like 45 controls that I look at to make sure that they're in place, and they're working as designed."

Controls can be everything from having a viable reporting mechanism to surveillance equipment to access control. The "working as designed" is key, if the access control is easily or regularly bypassed, then it's more security theater than actual security.

"As you go through this process, you see what's implemented, what vulnerabilities you have, and from that you can make a plan to begin to address vulnerabilities based on what you can afford, and you ask yourself what's going to cause the most problems if we don't fix it?"

Gips said it was important to think about the composition of your threat assessment team. "The internal threat assessment team shouldn't just be your security team," he said. "I think it should be led by security, but you need to have a broad set of skills and competencies taking part. You should have people from different business units—people working in different areas are going to have different perspectives on threat vectors and what the vulnerabilities are. So having a multifaceted, diverse team, led by someone who can explain the principles of threat management, is really important."

One other factor to consider that came up several times in the conversations with security executives is how these cascading threats affect the security team in particular.

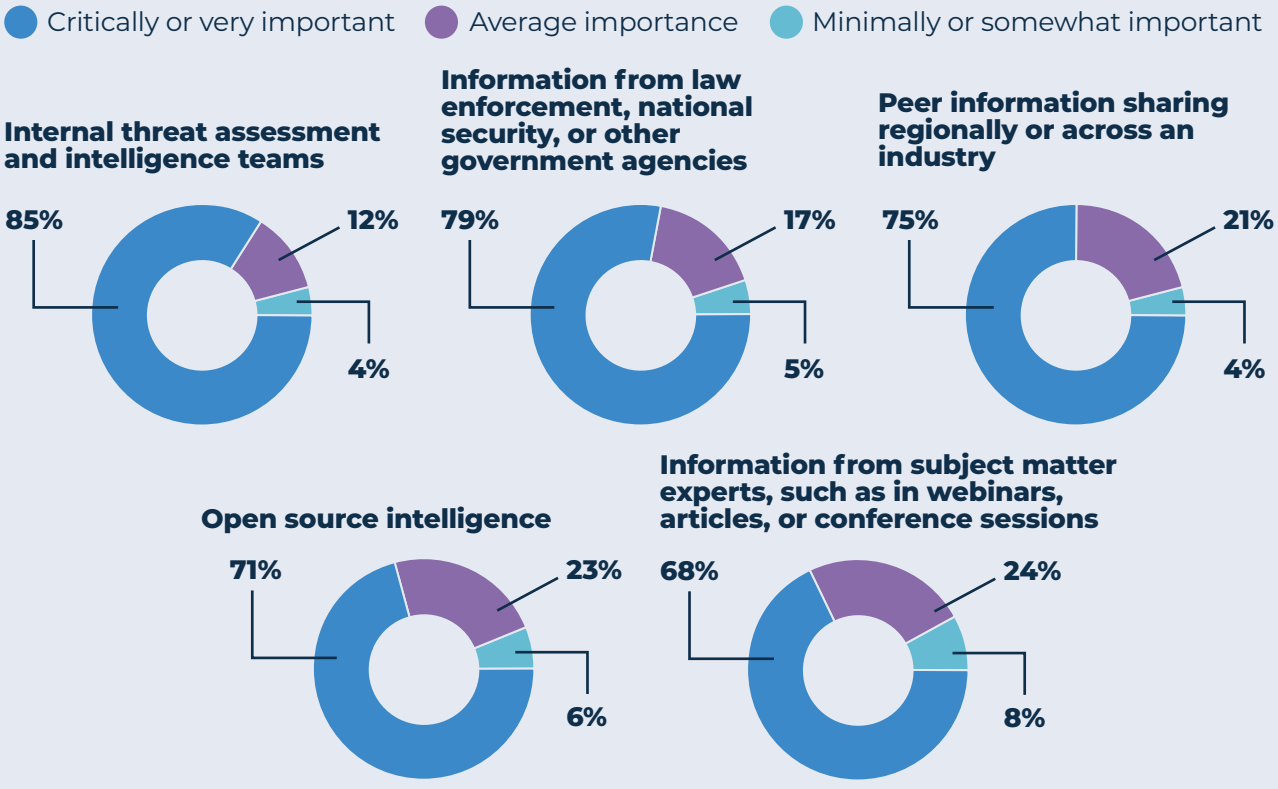
At the ASIS Europe conference, Gigi Agassini, CPP, a security consultant based out of Quebec, Canada, said she had several conversations with peers on mental health issues. "What happens when your crisis manager has a crisis?" she asked. "What is your plan B?"

Concannon said it is critical for security leaders to address this, both for their teams and for themselves. “By our nature, security professionals want to be there, want to assist” when there is a crisis, she said. “When there is a permacrisis, there is never a break—they don’t naturally happen. So we have to build [breaks] in, and we have to make sure we build them in for our teams… It has to be intentional in a way that I think is more important now than it ever has been before.”

Her advice is for security leaders to force themselves to take breaks, and to be visible about it, letting their teams know they are stepping back for a few minutes, and then being intentional in designing breaks for the entire security team. “Know your team,” she said. “We’re all different. Know who needs to sit out for a longer period of time and who needs short breaks on the hour…. That’s being meaningful, and that is what I think will support resilience.”

She also said security leaders must be aware of how the crises affects the wider organization. People have a heightened sensitivity to threats, and even people on the periphery of an incident need attention. “They may not be as capable sometimes as we might want them to be. They may be more reactive than we might want, and that results in them escalating situations that we’re dealing with,” she explained. “Their resilience has been compromised, so they feel very threatened even when the threat” to them may not be significant.

Figure 1.3: Importance of Threat Identification Methods



SECURITY LEADERS DO NOT HAVE THE INFLUENCE THEY NEED

"Security is an area of technical specialized activity and is not considered as a business enabler. This specialization means at a corporate level, security has a constrained degree of influence when compared to general managers who work across multiple business activity areas and demonstrate higher degrees of business influence. While security's operational activities span the organization, its risk management diagnosis activities are siloed, therefore giving an impression of broader influence than it achieves at senior decision-making levels."

That statement is from the ASIS Foundation study, *The Influence of Security Risk Management: Understanding Security's Corporate Sphere of Risk Influence,* published in 2023. The study gave several reasons for this lack of influence, chiefly:

- Executives see security risks as having only limited impact on the organization's strategic objectives.
- Cybersecurity is the one type of security risk that has made the jump in strategic importance, and it did so because of the high profile of cybersecurity failures.
- Security professionals have been unsuccessful in engaging with executive decision makers.
- Security may have a role in risk identification, but this is different than deciding risk treatment, and risk treatment, or what to do about the risks, is a more strategic, higher level business activity than security has obtained.
- Security as a business discipline lacks the professional respect that other disciplines command.
- Security professionals approach risk using the language of security, whereas decision makers approach risk using the language of business.

The just-completed survey set out to quantify security's lack of needed influence so it can be used as benchmarks for future studies. It also explored the effectiveness of techniques to close the gap between actual influence and desired influence. Finally, in the next section, this study examines some of the consequences of this lack of influence.

Anecdotally, this idea has been circulating in the security sector for decades. It is not hard to explain why that is, nor is it hard to explain why continued change is needed.

"Most people in an organization don't know what security folks do," Daniel Kennedy with Forensic Criminology Associates said in a focus group. "They think that security is the old guy at the gate with the sloppy uniform and white socks and big shoes, that's it. They don't understand that security is information. It's using intelligence to protect people, property, and information."

Gips, said one reason corporate security is tactical and reactionary rather than proactive and strategic is the profession's law enforcement roots. He knows there are law enforcement programs, such as community policing, that are proactive, however "law enforcement is by and large reactive. The job of the police is to respond to and investigate crime. So much of the corporate security world comes from that background

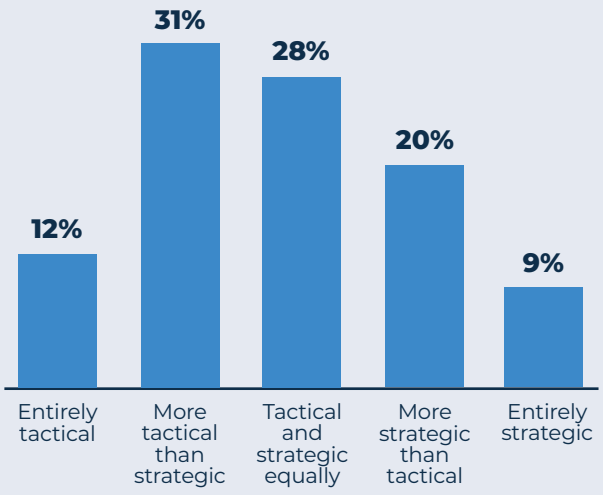
and they bring that with them. Now, some of the best CSOs and security practitioners out there come from that background. But they've taken that law enforcement knowledge and layered a knowledge of the business on top of it."

"Security in the private sector, compared to the public side, we have to show a return on investment," said Daniel Loo, CPP, regional practice leader, security risk consulting, with Telgian Engineering and Consulting. "We're not generating revenue or profit, so we have to show that ROI by mitigating risks, threats, vulnerabilities, etcetera."

Asked if the rest of the organization viewed security more tactically or more strategically, the survey results tilted tactical.

Referencing Figure 2.1, for security to build the influence it needs in risk decisions, the third column—tactical and strategic equally—and fourth column—more strategic than tactical—need to dominate the chart. Should those two columns combined approach 80 or 90 percent, compared to the current 48 percent, it would show security has broken through and gained the strategic influence it needs to properly incorporate security risk management into the organization's overall risk management approach. With all due respect to the nine percent who answered "entirely strategic," as Concannon said, "Security must attend to both"—there will always be an important tactical component of security

Figure 2.1: How Does the Organization View Security



"I don't think it is a matter of breaking through, I think it's a matter of accommodating both and living in both worlds in a way that is very complex: We're executing on the tactical needs and constantly being mindful of the strategy," she continued. "And the strategy evolves as we implement the tactics in a way that is extremely dynamic."

In the study, however, a combined 43 percent said that security is viewed either entirely or mostly tactical, which severely limits security's influence on more strategic issues including risk management.

Concannon noted that there is often a difference between how security approaches strategy and how other parts of the business approach it. "Other strategic elements of the business are a little bit more static," she said, noting three-year and five-year strategic planning models. "We are iterative in a way that others just aren't. ...When I look at a security strategic plan, I don't think five years. That just doesn't work in my world. [Security] is just so much more dynamic than that."

Moving on from examining the security function as a whole, the survey also asked related questions about the senior security executive specifically. Removing the small percentage who said they could not answer the question, there is a large dichotomy between how senior security executives spend their time and how survey participants said senior security executives should spend their time.

Only 18 percent of respondents said their senior security executive spent more than three-quar-

ters of their time on high-level or strategic planning. That compares to an ideal state that is nine points higher: 27 percent said the senior security executive should spend more than three-quarters of their time on high-level, strategic issues. (See Figure 2.2)

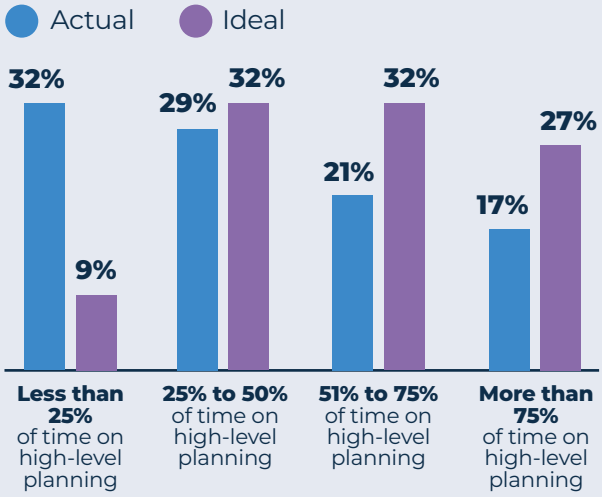
The other end exposes an even wider dichotomy: nine percent of respondents think the senior security executive should spend a quarter of their time or less on strategic issues. That compares to 32 percent who said the senior security executive actually spends less than a quarter of their time on strategic issues—that's a spread of 23 points between the ideal state and the actual state.

Agassini had a wonderfully simple suggestion to begin to address this dichotomy: update job descriptions.

"Everything starts through HR," she said. "The description of the job is very tactical, so of course companies are searching for a tactical person. It's important for other areas to know that the security person is not a policeman. It's not a person that is in charge of just surveillance, the cameras, the entrances. That is completely wrong. [Changing the perception] will be a process, and it has to start" by hiring someone with the skills—and mandated responsibilities—that can change the perception that the rest of the organization has about security.

A quick aside about the study's demographics: 19 percent of survey participants had titles of chief security officer or other chief-level positions (excluding consultants, industry partners, and those who listed "other"). Another 24 percent listed director of security or other director as their title, and while it's impossible to know exactly how many, a portion of these will be the senior security executive at their organizations. Another 16 percent had a title of senior manager of security. The point: Survey participants are likely to have reasonable estimates of the amount of time the

Figure 2.2: Ideal vs. Actual Time Senior Security Executives Spend on Strategic Matters



senior security executive spends on tactical versus strategic pursuits.

Because security risk management—as well as an organization's overall risk management program—involves proactive, strategic responsibilities rather than tactical, reactive actions, the survey results show that the status and responsibility areas of security leaders means they spend less than an ideal amount of time on the strategic issues such as risk management planning.

Focus group participant Vincent Soistier, managing partner, Interlira Risk Consulting, who is based in Brazil, described the issue matter-of-factly: "In my experience, the necessity of security starts when the company has a problem, it's not preventive. When they are confronted with a problem that they cannot manage, then they see that security is useful."

Another focus group participant, Jordan Caldwell, chief security officer at Critical Fault, said he's seen a lack of willingness to change on the

part of security. “One thing I’ve experienced is the physical security world is kind of like how computer security was 20 years ago, where a lot of it is reactionary and the industry doesn’t talk about the problems it has,” he said. “It’s very simple to install a solution and then say you’re done. …When I’ve tried to engage with security-implementing companies, they’re just not interested in hearing about things that are wrong and [how] they can go fix things. There’s a lack of willingness to go in and look at things proactively and really engage in that way. That promotes the idea that they’re just responders.”

Organizational status also goes hand in hand with budgeting authority. Security’s limited status means it is often scrounging for resources relative to other areas that executives view as mission critical.

“It all boils down to money,” said Kennedy. “Management pays attention to profit centers, so when security is seen as just a cost center, it won’t get the attention. But if you can show management that security is not just a cost center, that security can actually make money, then you can change attitudes about security. A quick example: in the retail industry, you might have a small profit of two or three percent, and you might have a shrinkage rate of six percent. If some investments in security could cut shrinkage in half, you’ve doubled your profits. …Think about how much one security incident can cost. I remember a case I worked at a Ford Motor plant… people were talking about a shooting at this plant that had occurred over 10 years prior to the event that brought me there. These events, if they hit the papers, they can [affect] your company for years and years afterward.”

It’s one thing to highlight the issue of security’s organizational limitations. The ASIS Foundation report on security’s risk influence does an excellent job describing the situation and offering pathways for improvement. That work, by-and-large, used research methods to record and articulate the thousands of conversations security leaders have been having for decades.

One of the goals of this research project was to examine the foundation project’s recommended pathways for improvement, which included actions such as working to get CEO buy-in, highlighting security’s value in times of emergency, and building rapport with executives from other disciplines. This research was able to provide some benchmarks, however, there is no panacea or magic formula that will take security leaders from their current state of influence directly to their desired state of influence. One obvious omission in quantitative explanations is the all-important, “How?”—how to accomplish the things being recommended.

It is somewhat useful, for example, to have data backing up the assumption that gaining CEO or executive committee support has an overwhelmingly positive effect on security’s ability to contribute in areas of strategic importance. How a security leader who lacks influence with this important group is supposed to gain such support is not quantifiable via survey. Some of the focus group discussions add qualitative insight into the “how” questions, but again, do not expect a neat, step-by-step answer.

With that preamble, here is what the research showed about methods to redefine security’s role to one that is highly strategic as well as tactical.

The survey asked respondents to rate the importance security has in their organization’s overall risk management function: 73 percent rated it as very important or important (what we’ll call high influencers for the rest of this section) and 27 percent rated it as somewhat important, of limited importance, or not at all important (low influencers). High influencers and low influencers were then asked separate, but related questions.

The high influencers were presented with six methods security leaders could use to gain status—methods derived from the ASIS Foundation study—and asked which of those contributed to security having the importance it had in risk management. Low influencers were asked if they had tried to use the methods to increase the role security played. Figure 2.3 shows the results.

Right away it is noticeable that CEO or executive committee support is at the top of the list of factors that contributed to security's influence, and it is closer to the bottom of the list of techniques that those with low influence had tried. As alluded to previously, one likely reason for the disconnect is that many security leaders will lack a practical means of accessing the CEO or executive committee—the "How?" question.

Jeff Ashley, CPP, the head of security at Nexteer Automotive in Auburn Hills, Michigan, fell squarely in the category who had increased security's role in risk management as a result of a restructuring. "One of the points I brought up—and it was very controversial," said Ashley, "was how can I report to HR or operations or the CIO if I'm doing threat assessments on their processes? It's very difficult to do, so I needed separation from that, to be independent, so I could give them a true understanding of where their processes are broken or need to be fixed." The restructuring put Ashley in the legal department.

The focus groups zoned in on the two techniques that led the way for those who lacked importance in risk management decisions: building trust with executives in other departments and taking advantage of incidents to highlight the value security can bring to strategic risk decisions.

Jim Hansel, director of corporate security at Insperity, described how he transformed a security function that was entirely reactive and tactical into one that built in proactive security strategies. "Four years ago when I came to this company, and they're a multi-billion dollar company, they had *a* security guy." The person oversaw the contracted security at the company's corporate campus in Houston. "Meanwhile, at the time we had about 80 remote sites throughout the U.S. that were basically just left unattended from a security perspective."

He called the security team the "fire department," because all they did was wait for something to happen and then they would go deal with it. "When something was happening, when something was on 'fire,' the security team came out and put out the fire, and then they went back to eating pizza and kolaches and waited for the next call to come in."

To get away from the fire drill method of security, he used security's tactical expertise to build relationships, and from there built more strategic roles for security. "We did it by building relationships within the company, by reaching out to stakeholders who are having problems with workplace violence issues, who are having problems with access, who can't see their camera systems and have a business need to secure PII [personal identifiable information]."

Helping solve those problems was the relationship builder. "It was tactical at first, but we had a stretch goal of becoming a strategic program." The next step for Hansel and his team was to understand what was important to the business units. "To me it was about solving problems in business, enabling business." As they learned more about a department's business needs, they were able to "go in and say, 'Hey, we're going to make this process better for you.' They begin to see you as a business enabler instead of a roadblock to be overcome.

"Once we started that," he continued, "we started to get a seat at the table. We got invited to other meetings because we were problem solv-

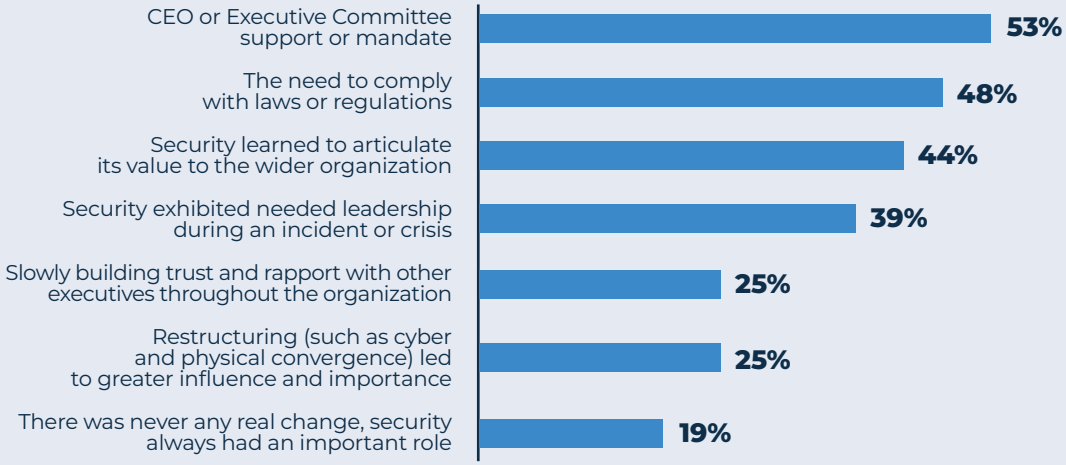
ers. The more you talk to people, and understand their needs, the more you get their buy-in. It started at the manager level, and then it was the directors and then vice presidents. Next thing I know, I'm called into a meeting with the CFO and all of these people who outrank you are in the meeting, and they're asking for your input."

To build influence with other executives from other departments, Agassini said, "Stop talking and start listening. What is your responsibility? Your responsibility is to help them achieve their goals. Understand the needs they have. What are the critical things they do? It's not about you, it's about how you will be a helper, a key person and advisor for them to help them achieve the goals they have."

Concannon built on this idea: "Each department has its priorities and its challenges—the things they find that are putting what they're trying to accomplish at risk. Some of those [challenges]

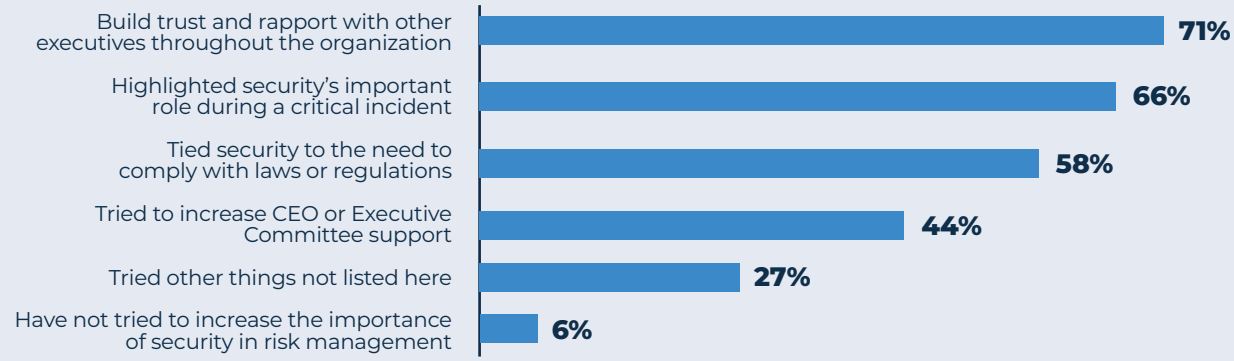
Figure 2.3: Methods to Enhance Security's Strategic Role

Factors that contributed to the importance of role security has in risk management



This question was answered by respondents who said security had either a very important or important role in risk management.

Techniques attempted to increase the importance of role security has in risk management



This question was answered by respondents who said security had a somewhat important, of limited importance, or not at all important role in risk management.

are areas that security has incredible expertise in, and that's where those partnerships can form. I think security sometimes underestimates what it can contribute in those spaces. It's not transactional as much as interpersonal. ...Once those interpersonal relationships are formed, that's when things transform."

Several security professionals in the focus groups advocated taking advantage of incidents when they happen—both at the organization or at other organizations in the same sector.

"You can get the CEO's attention briefly when something happens at another hospital that is similar to their [hospital], or to any kind of organization that is similar, whether that's a retail store or government agency or whatever," said Ramsey-Hamilton. "When there's a high-profile incident that happens, everybody goes back and looks at what they're doing... and that's the best time to go in and try to talk to people and get that going."

She continued: With some senior executives "if you make an appointment and you go in and show them an incident log of all the things that have happened, they'll say, 'Oh, I didn't know we were out of compliance.' They might not know the general duty clause that says the employer is required to keep a safe workplace for employees and they might not know that it applies to them. I've done that in the past, and the CEO heard it, he told me to make a list of everything the company wasn't complying with and fix it. So there are ways to get to those CEOs."

So while there is no magic formula, the findings point to some of the important variables that can contribute to a workable formula. It is likely to be a long game, with successes and setbacks, and it takes planning and opportunism—and copious amounts of perseverance.

Security professionals who want to change perceptions of their departments and expand the strategic value of their departments should use these findings and the ASIS Foundation report to formulate a plan of action. Every situation is going to be unique. There is nothing Machiavellian about trying to understand the power dynamics in an organization and then using them to increase the importance and sphere of influence of security. Ultimately, organizations that embrace security's strategic role in developing organizational risk management plans will be safer, more secure, and more productive than those that do not.

MAKING SECURITY RISK MANAGEMENT EFFECTIVE

If the previous section was somewhat humbling for security professionals, fear not. In this section the report will highlight the many ways security risk management is working well, and it will analyze the factors that make security risk management most effective.

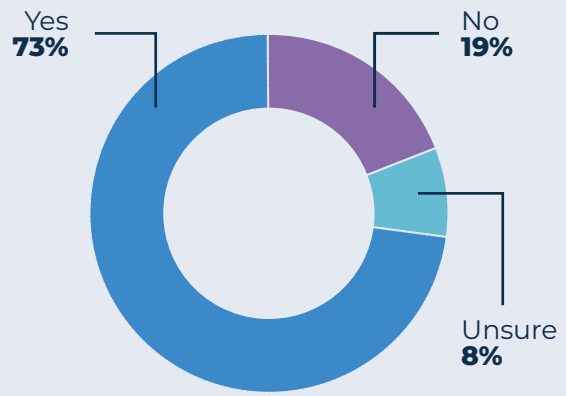
One caveat that applies to this entire section, and will be reiterated in the next section on enterprise security risk management (ESRM), is that the survey was promoted almost exclusively to ASIS International members and customers, who are overwhelmingly higher level security executives. The promotions noted the survey was on security risk management, almost assuredly leading to a self-selection bias, resulting in survey respondents highly likely to have advanced security risk management knowledge and practice compared to the overall population of security professionals.

Even with that bias, it is encouraging that 73 percent of respondents said their organization had a formalized risk management process.

As a quick quality check, the survey asked those security professionals who said they had a formal security risk management process if that process included a list of key assets, risks associated with those key assets, and associated risk mitigation measures—basic components of security risk management. Eighty-nine percent said their formal process had these components.

In another check, participants identified how they categorized risks. Forty-nine percent said it was a combination of asset value and the severity of the threat, 42 percent based it primarily on the severity and likelihood of the related threat, and five percent based it primarily on the value of the asset.

Figure 3.1: Have a Formalized Security Risk Management Process



Likewise, 81 percent said a significant incident would trigger a review of any affected risk assessments and mitigation measures. Asked to estimate how many times in the previous year an incident led to a change in a risk assessment or a risk management plan, 385 participants gave a response. The average number—4.6 times—skewed high with three estimates that were triple digits. The median number of 2 is more likely a better benchmark. In fact, 88 percent of security professionals had five or fewer reviews that led to risk plan changes, and 35 percent reported one or zero incidents.

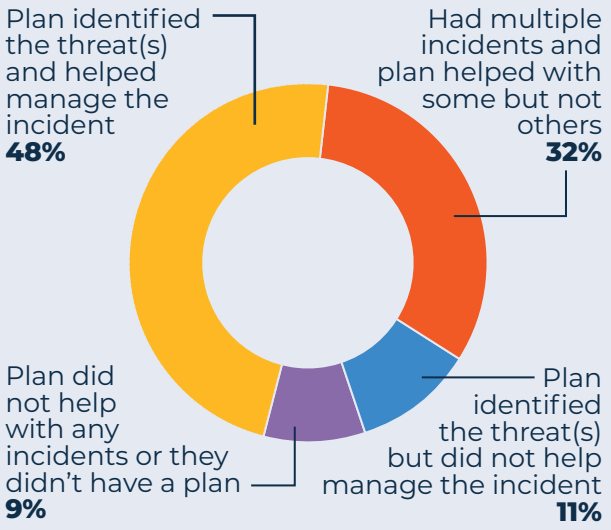
The previous section on threat identification noted that 75 percent of security professionals said they had experienced a serious incident in at least one of 11 categories (see Figure 1.2). The survey followed with a question asking if

the organization's risk management plan had identified the risk and helped the organization manage the incident. Respondents were given four choices:

- That the plan had identified the threat(s) and helped the organization manage or mitigate the incident.
- That the plan had identified the threat(s) but did not help the organization manage or mitigate the incident.
- That they had multiple incidents and the plan helped in some cases but not others.
- That their plan did not deal with the threat(s) or that they did not have a risk management plan.

As Figure 3.2 shows, 80 percent of security professionals reported that their organization's risk management plan had helped the organization manage or mitigate an incident that had a significant impact on the organization's operations, profitability, or reputation. In fact, at almost half (48 percent) of the organizations, the risk management plan had a perfect record of identifying the threats that led to the significant incidents and helped the organization manage the incident.

Figure 3.2: Did the Risk Management Plan Help Manage Significant Security Incidents?



Digging further into the data, it is possible to discern which types of incidents risk management plans were more successful at helping organizations mitigate. Asking about the effectiveness of the risk management plan for each individual type of incident would have made the survey instrument too long and complex. Instead, the survey broke the incidents to one set of five external factor categories (natural disasters or climate change, supply chain disruption, general civil unrest, civil unrest directed at the organization, and terrorism or war) and one set of six internal factor categories (compliance failure or breakdown, organized crime activity, workplace violence or active assailant, major property or intellectual theft, ransomware or other cyberattack, and kidnapping, extortion, or other executive protection issue).

Looking at each of those individual categories, researchers counted the number who had experienced an incident in a particular category and who said their risk plan helped manage the incident and compared it to the number of respondents who experienced an incident in the category and said their risk plan had not helped. (All mixed results were eliminated from the counts.)

The result yields a ratio of times per category that the risk plan helped compared to times it did not. According to these comparisons, risk management plans were most effective at managing terrorism or war and general civil unrest incidents. Risk plans were least effective at helping the organization manage compliance failures and major property or intellectual theft incidents.

Figure 3.3 presents the ratios for 10 of the incident categories—kidnapping, extortion, or other execu-

tive protection issues had too few instances for the results to be statistically meaningful. Read the ratio this way: For every organization that experienced a terrorism incident in which a risk plan did not help an organization, 3.21 organizations that experienced a terrorism incident did have a risk plan that helped the organization manage it.

Figure 3.3: Risk Management Plan Effectiveness Ratios

Type of Incident	Ratio
Terrorism or war	3.21
General civil unrest	3.00
Natural disaster or climate change	2.36
Civil unrest directed at the organization	2.25
Workplace violence or active assailant	2.21
Ransomware or other cyberattack	2.19
Supply chain disruption	1.81
Organized crime activity	1.75
Major property or intellectual theft	1.62
Compliance failure or breakdown	1.27

To find what factors contribute to security risk management effectiveness, researchers used the following survey question as the primary benchmark: "In the past year has your organization experienced a significant security incident that you think your organization could have realistically been better prepared to handle?" A total of 768 people answered the question, with 79 choosing "unsure" as their answer. The remaining 689 responses were very nearly split down the middle: 49 percent said yes and 51 percent said no.

A second effectiveness check was built into the survey by asking respondents to rank how effectively their organization manages risk overall on a 10-point scale, with 1 labeled "not at all effective," and 10 labeled "extremely effective."

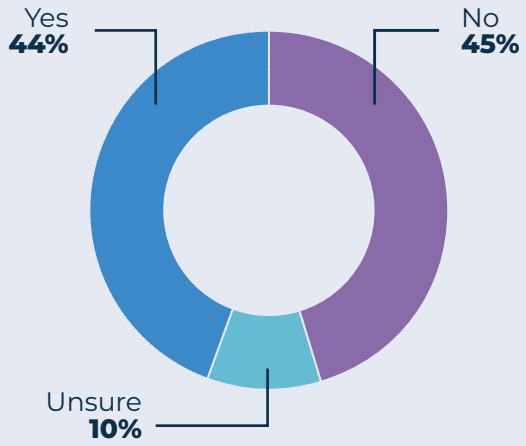
The average ranking was 7.06, so in this analysis, rankings of 8, 9, or 10 were considered better than average and rankings of 1 through 7 were considered worse than average.

The findings, for the most part, are unsurprising if not downright obvious. Still, it is beneficial to quantify the assumptions. For the rest of this section, we will examine three factors that the survey showed make a significant difference in the effectiveness of security risk management:

- Regularly re-examining the security risk management plan
- Security leaders who spend 50 percent or more of their time on strategic rather than tactical issues
- Security having an important role in the organization's overall risk management process

Most organizations revisit their security risk management plans regularly, but 1 in 10 said there is no set schedule, and they only revisit the

Figure 3.4: Did You Experience a Significant Security Incident You Could Have Been Better Prepared For?



plan when they determine it needs an update. Around 4 and 10 undertake a revision annually, 15 percent do so twice a year, and 22 percent have a quarterly process of revision. Another 12 percent said it was highly variable, and since this is not clear whether or not this meant it was revised regularly, these responses were disregarded in the effectiveness analysis. Finally, it should be noted that security professionals had the option of choosing "never," however no survey takers chose the option.

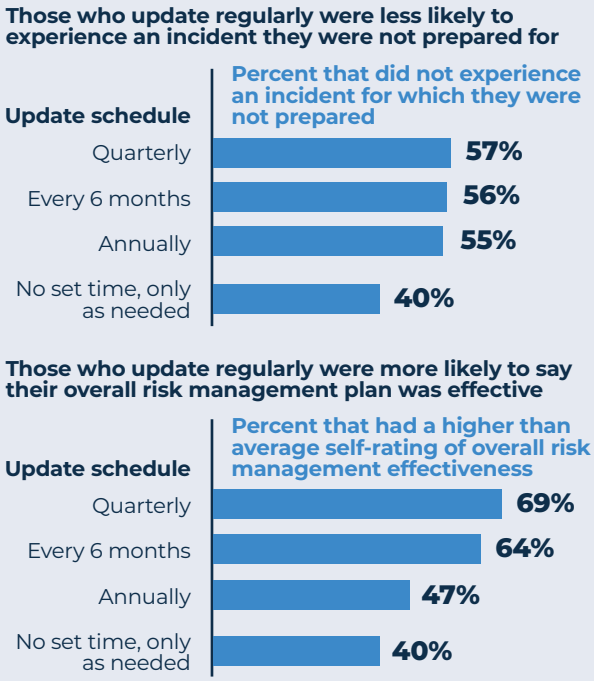
Comparing the frequency of plan updates with whether or not an organization experienced any significant security incidents that it could have been better prepared for yields Figure 3.5. The analysis showed no significant difference between the frequency of the regular updates, however, comparing those that do have a set schedule to those that do not clearly showed those with set schedules face fewer incidents for which they were not prepared than those without set schedules.

Comparing plan update frequency to rankings of overall risk management effectiveness affirms the relationship between having regular updates and effectiveness: 69 percent of those who update quarterly had better than average ratings on their organization's overall risk management effectiveness versus only 40 percent of those who did not update regularly.

"What I like to do," said Ashley, "is in January I present a perspective to the global operating committee on what that year's forecast is for intelligence, geopolitical events, or legal or regulatory things coming out—anything that could affect the company. It gives them a chance to step back and think about these things differently."

He said they will often pick up on a part of the presentation and dive deeper into one area. He also said that while he has the one annual chance to communicate directly with the board

Figure 3.5: Updating Security Risk Management Plans Regularly Makes Organizations More Effective at Risk Management



for an extended period of time, he supplements that with semi-annual or quarterly updates.

A previous section highlighted several findings that described the role security leaders have within organizations and asserted that in many cases, their sphere of influence had an adverse effect on their organization's risk management. The next two effectiveness arguments serve to quantify those assertions.

First, recall that the survey asked participants to rate how much time their organization's senior security executive spent on high-level, strategic activities versus managing day-to-day tactical activities. Sixty-one percent spent less than 50 percent of their time on strategy, leaving 39 percent who spent more than 50 percent of their time on strategy.

Comparing the time spent on strategy to whether or not the organization faced a security incident it could have been better prepared for did not yield informative results—the results essentially mimicked overall findings no matter how much time was spent on strategy versus tactical matters.

However, turning to how well the respondent rated the organization's risk management efforts, does show that time spent on strategy matters. Among organizations at which the senior security executive spends at least 75 percent of their time on strategic issues, one-third rated their organization's risk management effectiveness as either a 9 or 10 on a 10-point scale. That number tumbles to 14 percent for security professionals who spend less than 25 percent of their time on strategic issues. (See Figure 3.6)

Another factor that affects the effectiveness of risk management is the extent to which security has an important role in the process. The survey asked security professionals to rate how much importance security had in their organization's overall risk management function. The question gave a five-point rating scale, and nearly three-quarters chose either "4-Important: Secu-

Figure 3.6: Effectiveness of Organization's Risk Management Compared to Time Senior Security Executive Spends on Strategy

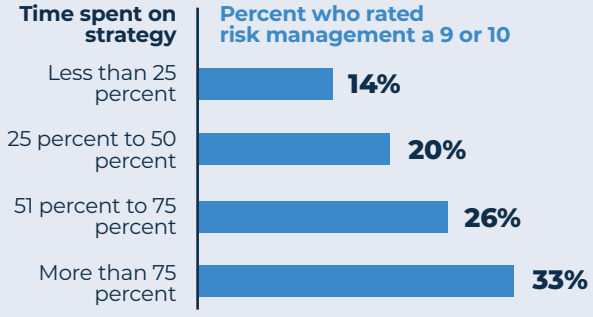
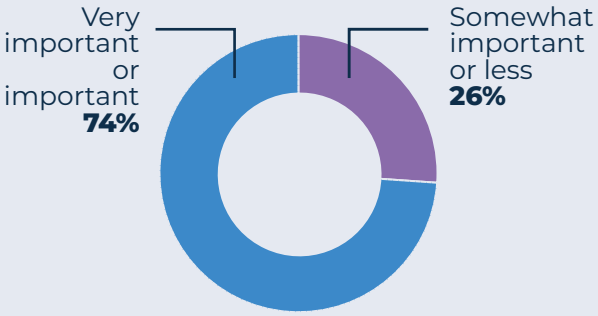


Figure 3.7: When Security Has a Major Role in Risk Management, It Improves an Organization's Overall Risk Management Effectiveness

How important is security in the organization's overall risk management function

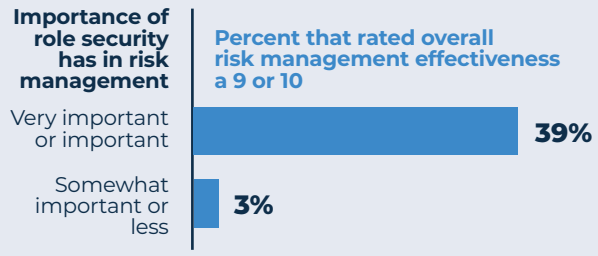


Importance of security compared to the number of incidents for which the organization could have been better prepared

60% of organizations where security plays an important role in risk management DID NOT EXPERIENCE a security incident in the previous year for which they were not prepared.

40% of organizations where security plays a less important role in risk management DID EXPERIENCE a security incident in the previous year for which they were not prepared.

Importance of security compared to overall risk management effectiveness



rity is one of the drivers of risk management" or "5-Very important: security is seen as critical in risk management." That left just over one-quarter choosing "3-Somewhat important: At about the same level as other departments" or categories with less influence.

For purposes of looking at effectiveness, researchers combined ratings of "important" and "very important" in one category, and those rated anything from "not at all important" to "somewhat important" in a second category. Both effectiveness measures showed that security having at least an important role had a positive impact on the organization's risk management effectiveness. When looking at incidents, 60 percent of respondents who said security had at least an important role in risk management did not experience security incidents for which they were not prepared. The inverse is true when security had less importance in risk management: 60 percent reported that they did experience security incidents for which they could have been better prepared. (Note: It is a coincidence that those percentages matched exactly.)

In addition, 31 percent of security professionals who said security had at least an important role in their organization's risk management function said that their organization was, overall, highly effective at risk management. That compares to just three percent of security professionals from organizations with a modest or no role in risk management. (See Figure 3.7)

THE EFFECT OF ENTERPRISE SECURITY RISK MANAGEMENT (ESRM)

Spoiler alert: ESRM has a positive impact on the results this research used to measure effectiveness. But before going there, it is important to note this was not a project designed to study ESRM specifically. ESRM is a specific way to approach security management that ties the security function into an organization's risk management planning. A key tenet is that owners of the assets needing protection are the final decision makers on how to protect their assets. Security provides input into the decision-making process, and the asset owners and security are jointly responsible for ensuring the needed protections are in place and working as designed. There is much more to ESRM than that, as reference see the ASIS ESRM Guideline.

A full study on ESRM would look very different than this research. However, since ESRM is such an important security business principle, and is clearly related to the discipline of security risk management, ASIS could not study the latter without at least touching on the former.

The survey asked consultants and security industry suppliers to answer two questions about ESRM and the results are presented here. Please note, the Methodology section gives additional details about the consultant component to the survey.

In addition, the survey asked security professionals a single question on ESRM: "Does your organization use enterprise security risk management (ESRM)?" They were given five answer choices ranging from "We fully embrace and implement ESRM across the organization," to "I am unfamiliar with ESRM or we do not apply ESRM concepts in my organization." (See Figure 4.1)

Overall, 23 percent of security professionals report that they have fully implemented ESRM and another 16 percent said they have embraced all or most of ESRM and are working to implement it. It's safe to say, a combined 40 percent having fully implemented or working toward full implementation of ESRM would be a surprisingly high percentage. Reiterating the previous cave-

Figure 4.1: Degree of ESRM Implementation

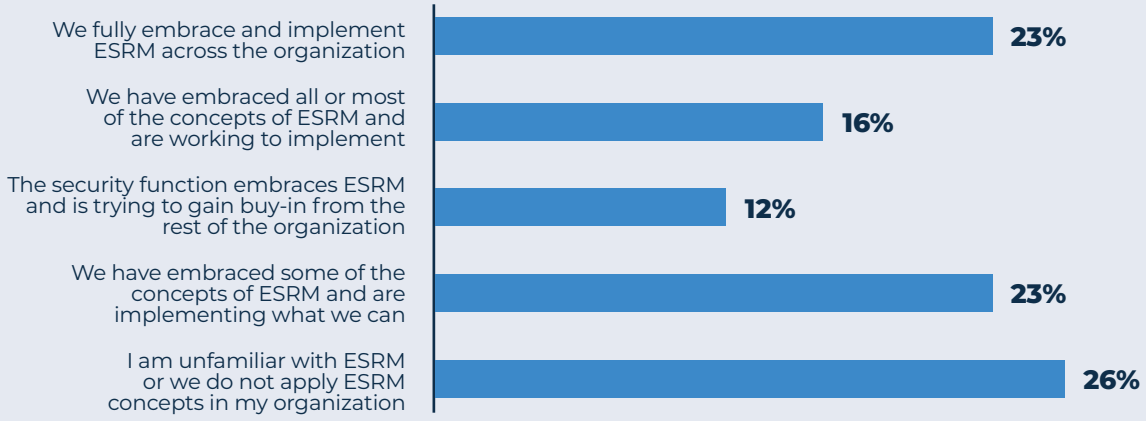
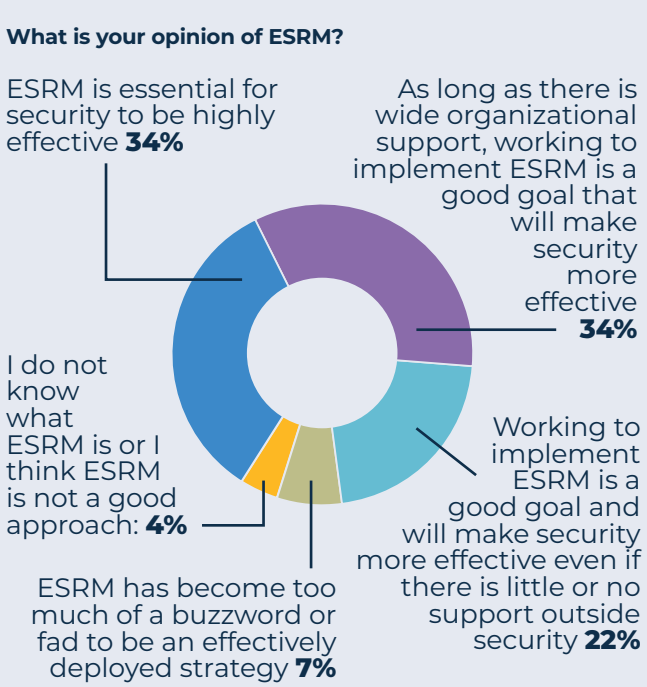
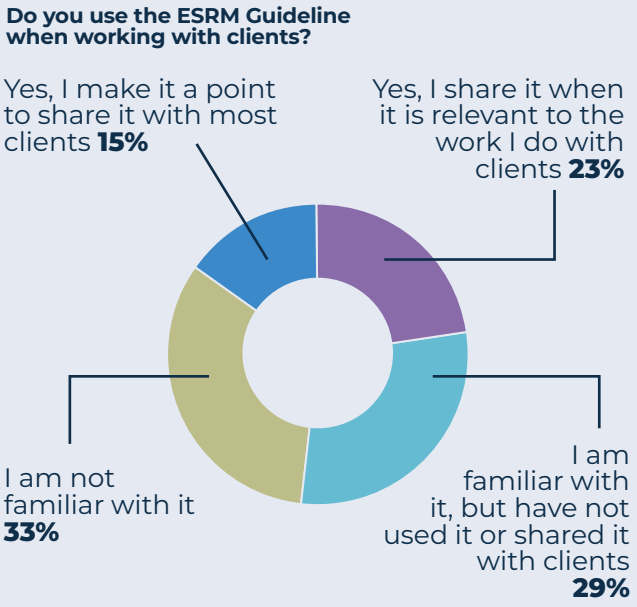


Figure 4.2: Security Consultants and ESRM





at: This survey was primarily promoted to ASIS members, which is a subset of all security leaders, and a subset more likely to be familiar with and aspire to ESRM. Furthermore, this research was promoted as being on security risk management, so, again, it is likely to attract responses from people interested in that topic.

And if the caveat alone does not explain what is, at glance, a surprising number, it is at least safe to assume that the 40 percent of respondents who said they fully implemented or were working toward full implementation have at least put forth some effort in embracing and implementing ESRM. So comparing this group to all the others can still yield meaningful comparisons.

"ESRM is a great model that I think is taking security from that tactical level to the strategic level," said Loo. "It's a broad, holistic approach and it explains security and security's role in a way that makes sense to the C-suite. In the grand scheme of things, it's still fairly new, so there's a lot of room for it to spread wider and have a significant impact, both for security as a profession, but also for companies overall."

In looking at effectiveness measures, organizations that have embraced ESRM have a positive, but small, correlation to having fewer security incidents for which it could have been better prepared: 62 percent to 55 percent (see Figure 4.3).

However, the correlation between ESRM and the perceptions security professionals have about their overall risk management effectiveness is much stronger. Four in 10 respondents who said they have either fully implemented ESRM or have embraced it fully and are working on full implementation rated their organization's overall risk management effectiveness as a 9 or 10. That compares to a 9 or 10 ranking from only 20 percent of respondents who are lower on the ESRM implementation spectrum.

Ashley, from Nexteer Automotive, said working to incorporate ESRM at Nexteer is how he was able to move the needle—both in terms of making security a more strategic function as well as getting access to senior executives.

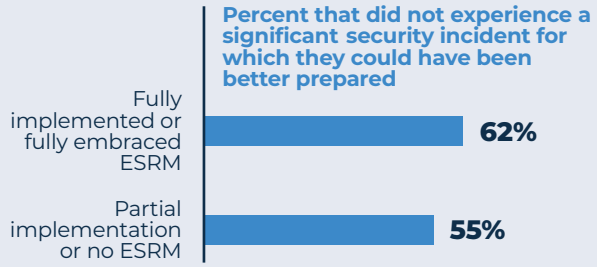
"What I did was: I took an ASIS presentation on ESRM and basically I stole it shamelessly, changing a little bit here and there to make it apply to my situation, and I was able to present it to our president and CEO," he said.

He could see that he was making progress. When he started, he reported up through human resources, but through "many presentations and a lot of politicking" he was able to engineer a reorganization where he reported to the company's general counsel, giving him more direct access to the board of directors and the global operating committee.

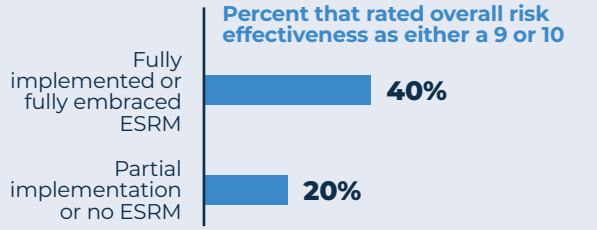
"Traditionally over the years the only time the C-suite would see us is when there was a crisis—a 9/11 or COVID—which kind of painted you into a tactical box. It was critically important to get that exposure outside of a crisis. So I would look at the context of whatever the company was making decisions about and talk about what that looks like form an ESRM perspective. Say they were looking at supply chain concerns and they're looking at it as part of ERM [enterprise risk management]. They're thinking about shortages and what that would mean, and I'm able to step in and talk about supply chain security and explain how I fit into that. I did that with a lot of the concerns they had in the ERM model, where I was able to pick up some of the areas they were looking at and carry them a lit bit further."

Figure 4.3: Positive Effect of ESRM on Risk Management

ESRM adoption compared to organizations that experienced incidents for which they were not prepared



ESRM adoption compared to ratings of overall risk management effectiveness



The results from the survey reinforce the notion that ESRM as a business practice holds great potential for security. The same methods covered in a previous section on how security professionals can work to be more strategic also apply to how security professionals can gain buy-in for ESRM. Indeed, as Ashley experienced, ESRM can be the basis for driving those methods.

METHODOLOGY AND DEMOGRAPHICS

This research project commenced in February 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, LifeRaft. The volunteer group shaped the survey questionnaire, which was deployed in March 2024. It consisted of a total of 48 questions, however, not every participant answered every question depending on how they answered previous questions. 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.

Overall, a total of 1,082 people answered at least some of the questions, and 817 completed the last question available to them. Data presented includes all data for that question, whether or not the survey was completed. Of the 157 consultants and business partners who participated, 92 (59 percent) opted to take the optional consultant survey. The consultant survey was used to look for themes for this final report, however, other than in the ESRM section, direct data was not presented. Results from the consultants' part of the survey will be part of an additional reflection on this project that will appear on ASIS International's *Security Management* website.

Several questions in the security professional section included additional branching, where only certain survey takers saw the question depending on how they answered a previous question. (For example, people who said they had explicit security risk management plans were asked how often they updated the plan, while those who said they did not have security risk management plans skipped that question.)

Most questions in the security professional part of the survey had more than 750 responses. That yields a margin of error of ±4 percent at the 95 percent confidence level. Some of the branched security professionals that not all participants saw had as few as 425 responses, yielding a margin of error of ±5 percent. The lowest number of responses in the consultant's survey was 78, yielding a margin of error of ±11 percent.

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.

Facility Scope	
Multinational with a variety of facility types in multiple countries	29%
Variety of facility types in multiple regions or locations, primarily within single country	29%
Multiple facilities primarily in a single region	26%
Mostly a single facility or single campus with a few facilities	17%

Region	
North America	47%
Central America, South America, Caribbean	9%
Europe	8%
Middle East	5%
Africa	16%
Oceania	3%
Asia	12%
Number of Employees	
1 to 100	19%
101 to 1,000	27%
1,001 to 10,000	28%
10,001 to 50,000	14%
50,001 to 100,000	5%
More than 100,000	7%
Industry	
Amusement, gambling, or recreation	2%
Banking, finance, insurance	8%
Consulting and professional services	10%
Defense and intelligence	4%
Education, K-12	1%
Education, university	3%
Emergency Services	1%

Food and agriculture	2%
Healthcare	4%
Hospitality and food services	3%
IT and telecommunications	7%
Law enforcement	4%
Manufacturing	8%
Media and entertainment	1%
Museums and cultural properties	1%
Oil, gas, chemical	5%
Pharmaceutical	2%
Public administration/government (nondefense, law enforcement, or education)	5%
Real estate and construction	3%
Retail	3%
Security services	18%
Transportation and supply chain	3%
Utilities	3%
Title	
CSO or VP of security	10%
CISO	1%
Other c-suite executive	3%
Director of security	15%
Other director (facilities, risk, compliance, etc.)	3%

Senior manager of security	13%
Manager of security	20%
Safety manager	2%
Other manager	4%
Frontline security	7%
Security consultant	13%
Nonsecurity role at business partner	2%

ADDENDUM: SUMMARY SURVEY RESULTS

Do other departments in your organization view security more as a tactical responder and operational function or more as a strategic partner and trusted advisor	
1 – Entirely as a tactical responder and operational function	11.9%
2 – A mix of both, but more tactical than strategic	31.4%
3 – Both about equally	28.0%
4 – A mix of both, but more strategic than tactical	19.9%
5 – Entirely as a strategic partner and trusted advisor	8.9%

n = 891, weighted average: 2.82

Please estimate how much time your senior security executive spends engaged in executive or strategic planning as opposed to managing day-to-day security operations.	
Less than 25% of the time on high-level planning	29.6%
25% to 50% of the time on high-level planning	26.9%
51% to 75% of the time on high-level planning	19.5%
More than 75% of the time on high-level planning	15.8%
Do not know	8.1%

n = 891

In your opinion, what percentage of time should the senior security executive spend engaged in executive or strategic planning as opposed to managing day-to-day operations	
Less than 25% of the time on high-level planning	8.7%
25% to 50% of the time on high-level planning	30.9%
51% to 75% of the time on high-level planning	31.4%
More than 75% of the time on high-level planning	26.6%
Do not know	2.5%

n = 889

What people or functions are heavily involved in your organization's overall risk management strategy? (Note: We are asking about all risk management, not just security risk management—please select all that apply)	
CEO	39.1%
CFO/accounting and finance	29.0%
COO	28.1%
Legal or regulatory compliance	47.9%
Security (physical security)	74.5%
Human resources	40.8%
IT or cybersecurity	56.8%
All or most members of Executive Committee (C-Suite)	31.4%
Safety or maintenance	41.8%
Facilities	36.4%
Risk management is decentralized, each function managing its own	24.8%
Risk management is not emphasized or is mostly ignored at my organization	6.6%
Other	5.5%

n = 893

Which functional area leads the overall risk management strategy at your organization? (If it is managed by cross-functional team, choose the function that leads the team.)	
CEO	15.6%
CFO	5.5%
COO	8.7%
Legal or regulatory compliance	9.5%
Senior security executive	25.6%
Senior human resources executive	1.9%
Senior IT executive	1.7%
We have a senior management position dedicated to risk management	23.7%
Other	7.7%

n = 633

Please rate the importance of security in your organization's overall risk management function.	
1 – Not at all important	0.4%
2 – Limited importance: Mostly limited to tactical security	7.8%
3 – Somewhat important: At about the same level as other departments	17.7%
4 – Important: Security is one of the drivers of risk management	22.9%
5 – Very important: Security is seen as critical in risk management	50.5%
Does not apply	0.7%

n = 459, weighted average: 4.16

Not asked to those who said security led the risk management function.

What rating do you think security should have in your organization's overall risk management function.	
1 – Not at all important	0%
2 – Limited importance: Mostly limited to tactical security	1.1%
3 – Somewhat important: At about the same level as other departments	4.8%
4 – Important: Security is one of the drivers of risk management	23.1%
5 – Very important: Security is seen as critical in risk management	70.7%
Does not apply	0.2%

n = 458, weighted average: 4.64

Not asked to those who said security led the risk management function.

Which of the following factors contribute to the importance of the role security has in risk management? (Choose up to 3)	
CEO or Executive Committee support or mandate	53.4%
The need to comply with laws or regulations	48.2%
Security learned to articulate its value to the wider organization	43.9%
Security exhibited needed leadership during an incident or incidents	38.6%
Slowly building trust and rapport with other executives throughout the organization	25.3%
Restructuring (such as cyber and physical security convergence) led to greater influence and importance	24.7%
There was never any real change, security always had an important role in risk management	19.2%
Do not know	1.2%

n = 490

Asked of those who said security had an important or very important role in risk management

Have you tried any of the techniques below to increase the importance security has in your organization's risk management function? (Choose all that apply)	
Build trust and rapport with other executives throughout the organization	70.8%
Highlighted security's important role during a critical incident	65.8%
Tied security to the need to comply with laws or regulations	57.5%
Tried to increase CEO or Executive Committee support	44.2%
I have tried other things not listed here	26.7%
I have not really tried to increase the importance of security in risk management	5.8%
Does not apply	2.5%

n = 120

Asked of those who said security did not have an important or very important role in risk management.

Which of the following threats present the most risk to your organization? (Choose up to 3)	
Workplace violence or active assailant	43.5%
Ransomware or other cyberattacks	41.9%
Property or intellectual property theft or destruction from an outside source	35.3%
Property or intellectual property theft or destruction from an inside source (or insider-assisted)	32.0%
Natural disasters or climate change	31.0%
Compliance failure or breakdown	30.4%
Organized crime activity	29.8%
Incidents that will disrupt your supply chain	28.0%
General civil unrest	23.7%
Terrorism or war	20.06%
Civil unrest directed specifically at your organization	17.2%
Kidnapping, extortion, or other executive protection issues	13.8%
None of the above	0.7%

n = 810

Please rate the importance of each of these threat identification methods					
Information from law enforcement, national security, or other government agencies, n=805					Weighted Average: 4.30
1 minimal importance	2	3 average importance	4	5 critically important	Do not use
1.7%	2.9%	16.8%	20.3%	57.9%	0.5%
Peer information sharing regionally or across an industry, n=804					Weighted Average: 4.15
1 minimal importance	2	3 average importance	4	5 critically important	Do not use
1.2%	2.9%	20.7%	29.7%	44.7%	0.9%
Open source intelligence service, n=801					Weighted Average: 4.03
1 minimal importance	2	3 average importance	4	5 critically important	Do not use
2.5%	3.9%	22.2%	29.6%	40.6%	1.3%
Information from subject matter experts, such as in webinars, articles, or conference sessions, n=804					Weighted Average: 3.89
1 minimal importance	2	3 average importance	4	5 critically important	Do not use
2.6%	5.4%	23.8%	36.0%	31.3%	1.0%
Internal threat assessment teams, n=803					Weighted Average: 4.42
1 minimal importance	2	3 average importance	4	5 critically important	Do not use
1.3%	2.4%	11.3%	21.5%	60.0%	3.5%

In the last year did you experience incidents in any of the following categories that had a significant impact on your organization's operations, profitability, or reputation?	
Natural disasters or climate change	25.3%
Supply chain disruption	23.4%
General civil unrest	21.3%
Civil unrest directed specifically at your organization	15.4%
Terrorism or war	13.0%
None of the above	41.9%

n = 795

Had your organization's risk management plan identified the risk and helped your organization minimize negative consequences from the incidents?	
Our risk management plan had identified the threat and helped us manage or mitigate the incident	54.4%
Our risk management plan had identified the threat but did not really help us manage or mitigate the incident	14.7%
We had multiple incidents, some of which were helped by risk management plans and some that were not.	21.2%
No, our risk management plan did not deal with that threat(s), or we have no formal risk management plan	9.7%

n = 463

Did not ask those who chose "none of the above" in previous question.

In the last year did you experience incidents in any of the following categories that had a significant impact on your organization's operations, profitability, or reputation?	
Compliance failure or breakdown	22.6%
Organized crime activity	20.1%
Workplace violence or active assailant	19.4%
Major property or intellectual theft	15.0%
Ransomware or other cyberattack	14.1%
Kidnapping, extortion, or other executive protection issue	6.0%
None of the above	44.6%

n = 788

Had your organization's risk management plan identified the risk and helped your organization minimize negative consequences from the incidents?	
Our risk management plan had identified the threat and helped us manage or mitigate the incident	47.6%
Our risk management plan had identified the threat but did not really help us manage or mitigate the incident	16.7%
We had multiple incidents, some of which were helped by risk management plans and some that were not.	26.1%
No, our risk management plan did not deal with that threat(s), or we have no formal risk management plan	9.6%

n = 437

Did not ask those who chose "none of the above" in previous question.

Does your organization have a formalized security risk management process?	
Yes	73.1%
No	18.5%
Unsure	8.4%

n = 789

Does your formal security risk management process include a list of key assets, risks associated with those key assets, and associated risk mitigation measures?	
Yes	89.0%
No	5.5%
Unsure	5.5%

n = 561

Only asked of those who had formalized security risk management process

What criteria do you use to categorize the level of risk?	
Primarily the severity or the likelihood of the threat	42.4%
Primarily on the value of the asset	5.4%
Equally or some combination of asset value and threat severity	48.7%
We do not categorize risk levels	1.6%

n = 561

Only asked of those who had formalized security risk management process

Does a significant incident trigger a review of risk assessments and mitigation measures?	
Yes	80.9%
No	10.2%
Unsure	8.9%

n = 561
Only asked of those who had formalized security risk management process

Estimate how many times in the last year an incident review resulted in a change to the risk assessment or risk management plan. Enter whole number	
Average	4.6
Median	2

n = 385
Only asked of those who had formalized security risk management process and had a significant incident that triggered review.

In general how often do you revisit your security risk assessments?	
Quarterly or more often	21.8%
Every 6 months	15.0%
Annually	40.1%
No set time, only when needed	9.7%
Never	0.0%
Unsure	2.2%

n = 559
Only asked of those who had formalized security risk management process

Does your organization use Enterprise Security Risk Management (ESRM)?	
We fully embrace and implement ESRM across the organization	22.8%
We have embraced all or most of the concepts of ESRM and are working to implement	16.0%
The security function embraces ESRM and is trying to get buy-in from the rest of the organization	11.7%
We have embraced some of the concepts of ESRM and are implementing what we can	23.2%
I am unfamiliar with ESRM or we do not apply ESRM concepts in my organization	26.4%

n = 557

Only asked of those who had formalized security risk management process

In the past year has your organization experienced a significant security incident that you think your organization could have realistically been better prepared to handle?	
Yes	44.3%
No	45.4%
Unsure	10.3%

n = 768

Estimate how many times in the last year an incident review resulted in a change to the risk assessment or risk management plan. Enter whole number	
Average	11.7
Median	2

n = 363

Only asked of those who had formalized security risk management process and had a significant incident that triggered review.

How do you communicate security risk management information to senior executives? (Choose all that apply)	
Written report, brief, or summary	76.9%
Meeting agenda item (live or conference call)	56.0%
Dashboard metrics	31.6%
Security risk management information is not communicated to senior executives	7.7%
Do not know	2.4%

n = 750

Please rate how much attention you think other executives give security risk management reports	
1 – Not nearly enough	13.0%
2	14.7%
3 – Usually enough attention	33.2%
4	12.9%
5 – They are highly engaged	25.0%
Not applicable	1.2%

n = 744, weighted average: 3.22

Have your threat mitigation measures successfully protected your organization from or during a specific threat or incident in the past year?	
Yes	58.5%
No	15.9%
Unsure	25.6%

n = 749

Please rate how effectively your organization manages risk overall.

Not at all effective									Extremely effective	
1	2	3	4	5	6	7	8	9	10	NA
1.6%	1.2%	2.7%	4.7%	10.2%	11.7%	20.7%	25.3%	11.0%	10.4%	0.4%

n = 738, weighted average: 7.1

Please rate how effectively your organization manages security risk.

Not at all effective									Extremely effective	
1	2	3	4	5	6	7	8	9	10	NA
1.5%	1.4%	3.1%	4.7%	8.6%	10.4%	18.5%	24.2%	15.5%	12.0%	0.1%

n = 742, weighted average: 7.21