ASIS INTERNATIONAL | SECURITY ISSUES RESEARCH

SECURITY INCIDENT MANAGEMENT IN 2025

RESEARCH ON HOW SECURITY PROFESSIONALS PREPARE FOR, RESPOND TO, AND RECOVER FROM SECURITY INCIDENTS

Sponsored by VOLT

Register now for the ASIS webinar on this research: 6 February 2025

CONTENTS

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

INTRODUCTION

In late summer 2024, ASIS International, with the support of VOLT, Inc., fielded a survey on security incident management. The goal was to get a better understanding of the policies, procedures, and technologies security professionals deployed to manage security incidents. Digging deeper, the survey sought to uncover what types of security incidents organizations faced and how prepared security professionals felt for those incidents. Finally, the study sought to identify factors that tend to lead to effective management of security incidents.

Perhaps more than some subjects, the research of security incidents is difficult because different types of organizations are going to face different types of incidents. At a retail store, a flash rob may be a significant security incident; college campuses have a volatile mix of young adults and intoxicating substances that can lead to a host of incidents; a technology company may be most concerned about theft of intellectual capital. While the survey did examine trends related to categories of incidents, the survey's guiding approach—which was developed by a small group of ASIS members who advised on the project—was to have survey participants make their own interpretations of incident descriptions.

For example, for one set of questions, participants were given the following descriptions:

- Low-Impact Security Incident: An incident that requires a security response but has little or no effect on short- or long-term operations, has little or no financial impact, or has little or no impact on the well-being of staff or other constituents.

- Medium-Impact Security Incident: An incident that possibly disrupts short-term operations or has a modest impact on long-term operations, potentially has a noticeable financial impact, or may involve compromised staff or constituent well-being.

- High-Impact Security Incident: An incident that may require crisis management, usually having a significant effect on operations, profitability, or staff or constituent well-being.

Even with the detailed descriptions, one security professional's medium-impact incident might be another security professional's high-impact incident. Likewise, using the research requires readers to assess for themselves what low-, medium-, and high-impact incidents mean at their organizations. The benchmarking and comparisons come with how organizations prepare for, respond to, and recover from incidents of varying severity regardless of the incidents themselves.

Overall, the work of managing incidents is integral to security. The management of incidents clearly includes preparing for incidents and recovering from incidents—which includes learning and adapting—are important considerations, and so the survey covers these areas in addition to covering incident response. Collectively, examining how security policies, procedures, and technologies enable effective preparation, response, and recovery actions can make organizations safer and more secure.

HOW THIS REPORT IS ORGANIZED

The report begins with what the researchers thought were the most interesting results from the survey analysis in a section called Key Findings. Often, research is about testing hypotheses, and some of these hypotheses are highly logical connections. Still, it is important to validate these logical connections with data.

The data supporting the key findings is presented in detail in the various sections that comprise the rest of the report.

The final section is "Methodology," which discusses the survey method and the demographics of those who took the survey.

KEY FINDINGS

KEY FINDING: READINESS LEVELS FOR HIGH-IMPACT SECURITY INCIDENTS LAG BEHIND READINESS LEVELS FOR MEDIUM – OR LOW-IMPACT INCIDENTS.

Overall, security professionals said they had the resources they needed for the number of incidents they faced and that they spent about the right amount of time dealing with security incidents. However, when examining the severity levels of different types of incidents, security professionals were much more likely to say they spent relatively too much time on low- and medium-impact incidents, and not enough time on high-impact incidents. Likewise, the percentage of respondents who said they had the resources to deal with each severity level was highest for low-impact incidents and lowest for high-impact incidents. (See the Security Incident Benchmarks section.)

KEY FINDING: ORGANIZATIONS ARE BETTER AT RESPONSE AND RECOVERY THAN AT ANTICIPATION AND PREPARATION.

To build resiliency, organizations need to be able to anticipate adverse events, prepare for them, respond to them when they occur, and recover from them effectively and efficiently. Survey respondents said their organization's ability to respond to medium- or high-impact incidents outpaced their ability to anticipate or prepare for them, with the ability to recover falling in between (see the Security Incident Benchmarks section). This finding is reinforced when examining the survey's technology-related questions. Response- and recovery-aligned benefits were realized more often than anticipation- and preparation-aligned benefits (see the Factors that Make Security More Effective at Managing Incidents section). However, note that this could be the case because the security technology studied aligns better with response and recovery and different technology beyond the scope of this research might align better with anticipation and preparation.

KEY FINDING: ORGANIZATIONS WOULD LIKE TO BE ABLE TO DETECT AND RESPOND TO SECURITY INCIDENTS QUICKER.

Almost nine in ten security professionals said they would like to make either significant or incremental improvements in how fast they detect and respond to security incidents. Only 13 percent said that, in general, they detect and respond to incidents quickly and any attempts to improve would likely be marginal improvements at best (see the Security Benchmarks section).

KEY FINDING: ORGANIZATIONS ARE BEST EQUIPPED TO HANDLE INTRUDERS AND PHISHING OR SOCIAL ENGINEERING ATTACKS; THEY ARE LEAST EQUIPPED TO HANDLE SENIOR EXECUTIVE KIDNAPPING.

From a list of eight types of security incidents, security professionals reported they are best equipped to handle intruders discovered in places they are not supposed to be as well as attempts at phishing or other social engineering. They said they were least equipped to handle senior executive kidnapping incidents (see the Security Benchmarks section).

KEY FINDING: AFTER-ACTION REPORTS FOLLOWING INCIDENTS ARE A CRITICAL SECURITY TOOL.

Almost all organizations—90 percent—create security incident after-action reports. Of those, almost all of them have used the reports to make

improvements to how they manage security incidents. The top action taken: using the reports to create security awareness materials or training. Organizations also used them to strategically redeploy security resources, and, importantly, to justify increased investment in security technology and personnel. (See the Learning from Security Incidents section.)

KEY FINDING: FACTORS THAT MAKE ORGANIZATIONS MORE EFFECTIVE AT SECURITY INCIDENT MANAGEMENT

How effective is your organization at managing security incidents? It's a difficult and necessarily subjective question. The survey asked the question directly, asking security professionals to rate their organization's effectiveness. These answers were crosstabulated with a lot of the security incident benchmarking questions to provide a look at what has the biggest impact on the confidence security professionals have in their ability to manage security incidents effectively. The results, as well as direct questions on how a particular technology aided incident management, yielded four critical success factors:

Critical success factor 1: Investing in security technology.

Critical success factor 2: Improving detection and response time.

Critical success factor 3: Running a security operations center 24/7.

Critical success factor 4: Creating and using security incident after-action reports.

SECURITY INDUSTRY BENCHMARKS

This section presents a lot of the data gathered in the survey, beginning with time and resource allocations for managing incidents and reviewing incident reports. It will provide benchmarks on organizational effectiveness in the phases of resiliency as well as the types of incidents security faces.

The survey instructed participants to consider the incidents they face and categorize them as low impact, medium impact, or high impact, given the following definitions:

- Low-Impact Security Incident: An incident that requires a security response but has little or no effect on short- or long-term operations, has little or no financial impact, or has little or no impact on the well-being of staff or other constituents.
- Medium-Impact Security Incident: An incident that possibly disrupts short-term operations or has a modest impact on long-term operations, potentially has a noticeable financial impact, or may involve compromised staff or constituent well-being.
- High-Impact Security Incident: An incident that may require crisis management, usually having a significant effect on operations, profitability, or staff or constituent well-being.

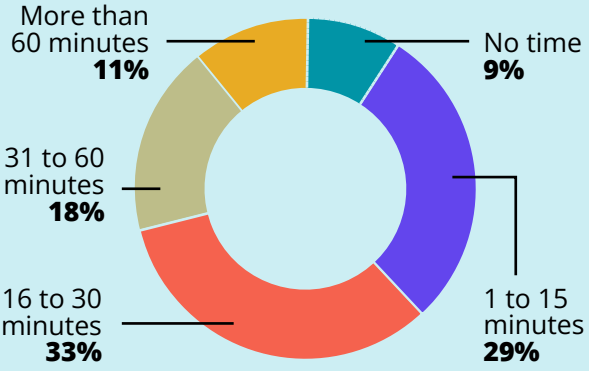
Even with the detailed descriptions, one security professional's medium-impact incident might be another security professional's high-impact incident. Furthermore, demographics of the survey participants are presented in the Methodology section, but it's important to consider that the responses are from all manner of different types and sizes of organizations. A security professional at a small manufacturer likely considers security incident management very differently than one from a Fortune 100-sized global manufacturing company. And a manufacturing company likely has vastly different security incident considerations than a museum or an insurance company, yet data from all these types of organizations is aggregated into these data trends. Using the research benchmarks, then, requires readers to assess for themselves how their organization relates to the survey questions being asked.

SECURITY INCIDENT TIME AND RESOURCE BENCHMARKS

A majority of respondents said they review incident reports for 30 minutes or less per day (71 percent), though 11 percent report spending more than an hour a day on average (see Figure 2.1). The amount of time spent reviewing incident reports remains consistent across both the size of the organization and the title of the respondent.

For each category of incident—low, medium,

Figure 2.1: Daily Time Spent Reviewing Security Incident Reports



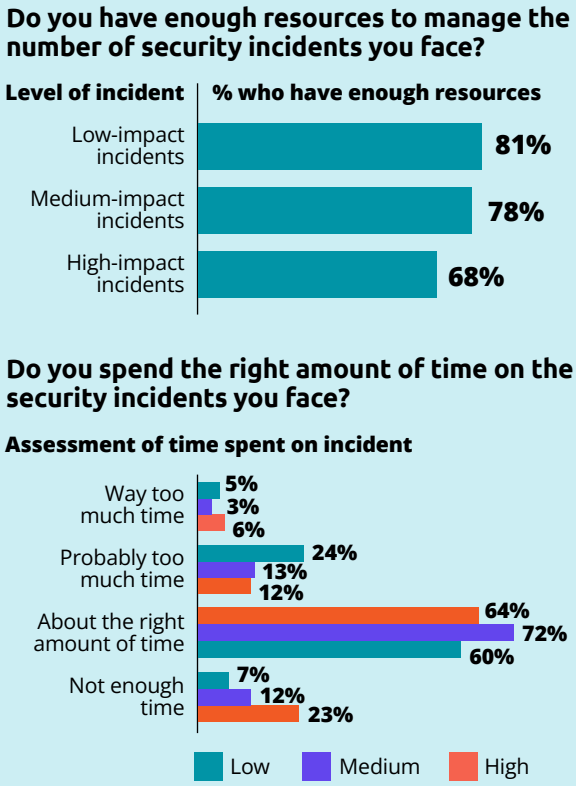
or high—the survey asked if their organizations both had the resources to deal with the number of incidents in each category, and whether or not they spend too much time on incidents in each category.

When it comes to actually dealing with security incidents, overall, security professionals said they have the resources they need to manage the number of incidents they face. However, there was a noticeable decline for high-impact incidents: 81 percent and 78 percent said they had enough resources for low- and medium-impact incidents respectively. That fell to 68 percent who said they had enough resources for the number of high-impact incidents they face (see Figure 2.2).

Similarly, the bottom chart of Figure 2.2 shows that security professionals generally think they spent about the right amount of time on each level of security incidents they face. However, the lowest set of bars shows that nearly a quarter of security professionals (23 percent) said they were not able to spend enough time on high-impact incidents—that is a significantly higher percentage than those who say the same for low-impact incidents (7 percent) or medium-impact incidents (12 percent).

Given the definitions they were provided, this is a disconnect organizations would do well to ensure they are addressing. High-impact incidents are the type of incidents that often lead to crisis management and are the type of incidents that executives and the board, and sometimes even the public, care about. Much of the rest of this report can be seen as a way to study how security professionals might best position themselves and their organizations to ensure they handle the low- and medium-impact incidents efficiently so that when high-impact incidents occur, they are in the best position to provide value to the organization by handling them effectively.

Figure 2.2: Management of Different Levels of Security Incidents



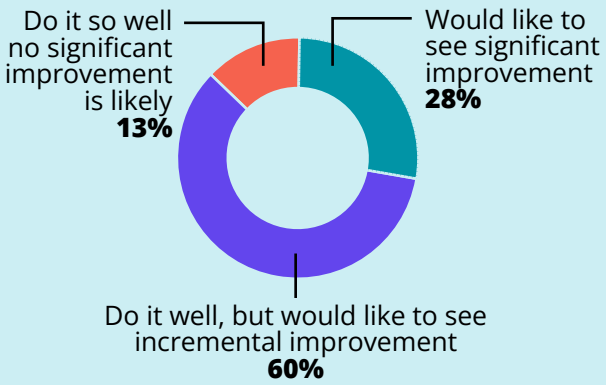
No matter how you look at security, being able to detect and respond to incidents quickly and decisively is a critical expectation. One of the key findings referenced an organizational resilience model that has four components: anticipation, preparation, response, and recovery (note: the full dataset regarding this organizational resilience model is the next section of the Security Incident Benchmarks section). The speed of detection and response is one of the ways that all four elements tie together. One of the key benefits of the anticipation and preparation elements is so that detection and response can be quick. And you want a quick response because that is your best chance to minimize negative consequences, which will lead to an easier recovery.

Another common way to think about physical security is the deter-detect-delay-deny rubric where the purpose is to deter an adversary, detect an attack, delay an attack, and deny an adversary access to its target. In the model, detection is one of the keys, and the quickness of response is what can delay and ultimately deny an attacker. So, it is no surprise that security professionals would want to do everything possible to increase the speed of their detection and response capabilities, and that's exactly what the research found.

The survey asked if security professionals were happy with their organization's security incident identification and response time. Almost nine in ten security professionals said they would like to make either significant or incremental improvements in how fast they detect and respond to security incidents. Only 13 percent said that, in general, they detect and respond to incidents quickly and any attempts to improve would likely result in marginal improvements at best (see Figure 2.3).

A final benchmark to examine in the resources section is the survey question asking about the effectiveness of specific security tactics. The question asked: "Which of the following do you deploy and what impact does it have on your incident prevention or response?" The tactics studied were: 24/7 staffing of a security operations center; lighting, fencing, natural or artificial barriers, or other crime prevention through environmental design (CPTED) techniques; weapons sensors at entrances; AI-enhanced surveillance to detect escalation or anomalies; and AI-enhanced surveillance to detect weapons.

Figure 2.3: Opinion of Time It Takes to Detect and Respond to Security Incident



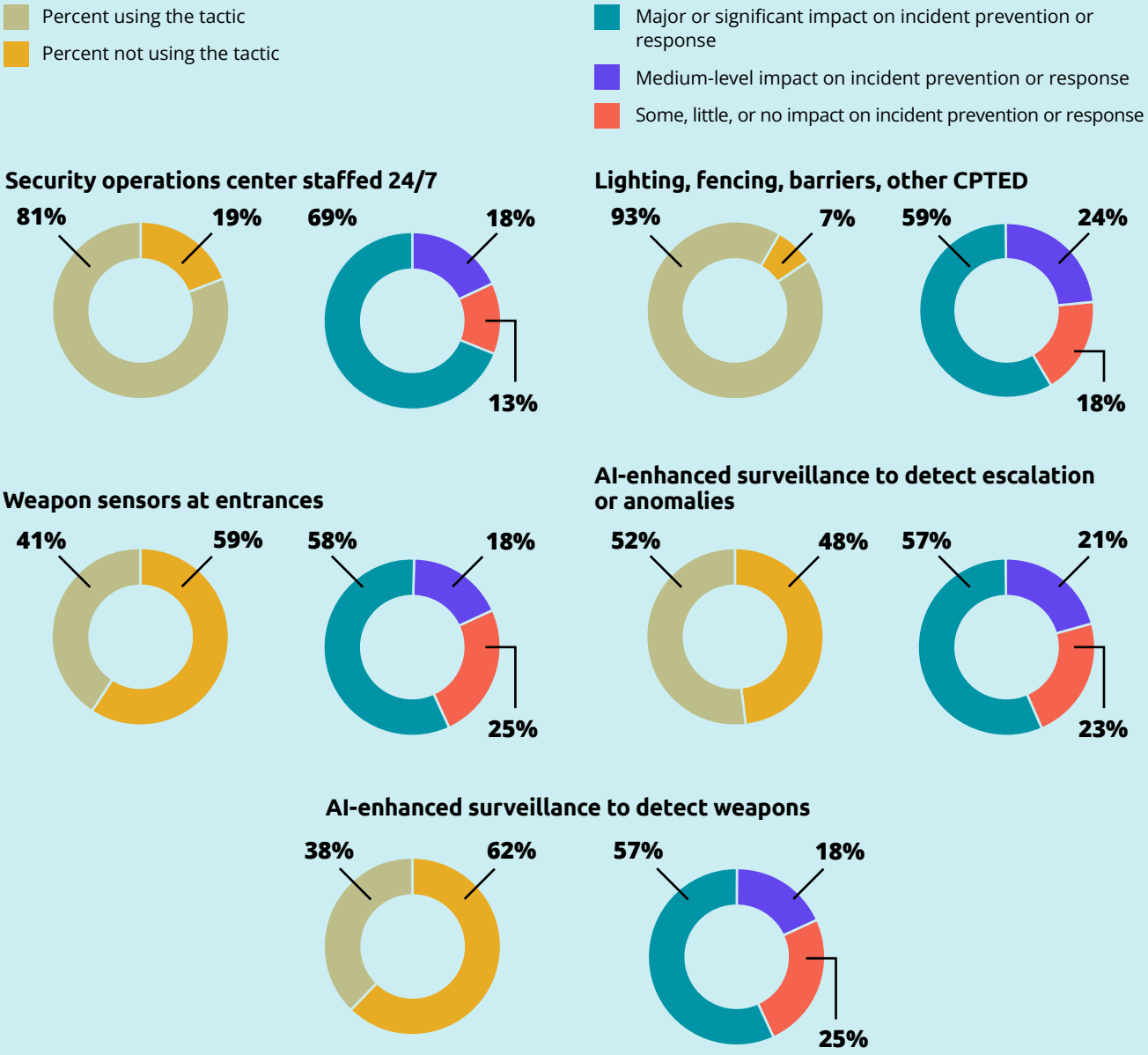
The first two tactics are more procedural or security design features while the last three deal with technology, a topic examined more closely in the next section. One noticeable difference is that far more respondents had deployed the procedural or design tactics than the technological ones (see the pie charts on the left in Figure 2.4). All of the tactics performed well—for each, a majority of security professionals who used the tactic said it had either a major or a significant impact (versus a little impact, some impact, or a medium-level of impact). Staffing a security operations center 24/7 led the way, with 69 percent saying it had a major or significant impact on incident prevention or response (see Figure 2.4).

ORGANIZATIONAL RESILIENCE

To build resiliency, organizations need to be able to anticipate adverse events, prepare for them, respond to them when they occur, and recover from them effectively and efficiently. Survey respondents said their organization's ability to respond to medium- or high-impact incidents outpaced their ability to anticipate or prepare for them, with the ability to recover falling in between (see Figure 2.5).

On one level, the findings are logical. Anticipating and preparing for security incidents involves the unknown. In planning for security incidents, no one can know exactly what kind of attack will actually occur, nor what vector that attack

Figure 2.4: Use and Effectiveness of Security Tactics



will take. Response is much more straightforward. While it can be chaotic, it is dealing with something that is happening, not something theoretical. When an incident occurs, security must respond.

Yet there is more nuance than just saying anticipation and preparation are more nebulous than response and so therefore are the harder parts of the resilience model. The survey asked about three general categories of security technology: access control, surveillance, and alarms. For those who had upgraded any of those systems in the past 18 months, researchers asked if they had experienced any of six benefits. Three of these benefits align more closely to the response or

Figure 2.5: Percent Who Consider Their Organization Above Average at Each Stage of the Resiliency Model Stages

recovery stages of the resilience model and three of them align more closely with the anticipation and preparation stages:

Response- and recovery-aligned benefits

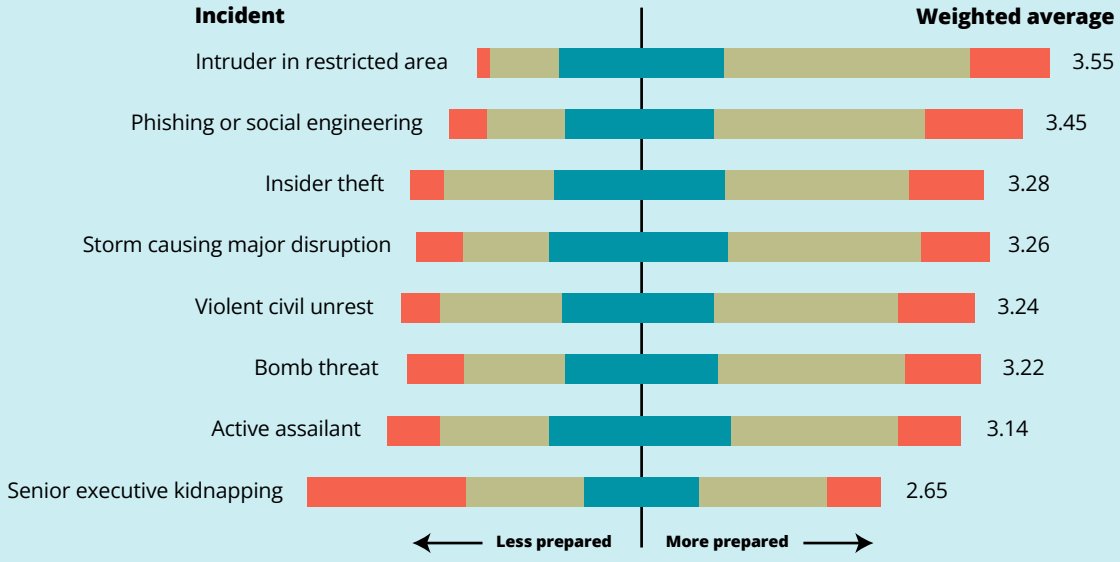
- Enable quicker or more accurate assessment of incident severity
- Enable quicker response to many incidents
- Enable better post-incident analysis

Anticipation- and preparation-aligned benefits

- Contributed to significantly fewer incidents
- Kept incidents from escalating
- Enable redeployment of security personnel to higher-impact responsibilities

Across all three categories of security technologies the research asked about, respondents said the upgrades had more response- and recovery-aligned benefits than anticipation- and preparation-aligned ones. This finding reinforces the notion that the primary security systems in use at most organizations are better at response and recovery than anticipation and preparation (see the Security Systems' Role in Incident Preparation, Identification, and Response section for more detail). Note, however, it is unknown if this is because security professionals chose to focus their security technology

Figure 2.6: How Well Prepared an Organization Is to Detect and Effectively Respond to Various Incidents



use on response and recovery because traditionally security is more aligned in those areas or because those systems just happened to be better equipped for response and recovery. The survey did not ask about other security technology that might align better with improved anticipation or preparation.

TYPES OF SECURITY INCIDENTS FACED

The survey gave security professionals a list of eight types of security incidents and asked them to rate how well they could detect and respond to each of them. Six in 10 respondents said they were either well prepared or highly prepared to detect and respond to an intruder in a restricted area. Security professionals also said their firms were well positioned to deal with incidents of phishing or other social engineering to gain IT access, with 54 percent being either well or highly prepared.

The type of incidents that security professionals felt least prepared for was a senior executive kidnapping: 32 percent felt well prepared or highly prepared for it, and 48 percent said they were not at all prepared or only somewhat prepared for such an incident. Respondents were also less confident in their ability to detect and respond to an active assailant incident than other types of incidents: only 40 percent felt well or highly prepared.

The other four types of incidents researchers asked about—insider theft, storm damage or disruption, violent civil unrest, and bomb threats—all scored roughly the same, with either 45 or 46 percent of respondents saying they were well or highly prepared to detect and respond to such incidents.

In conversations with researchers, security professionals noted that the complexity of security incident management has increased, with one reason being that incidents happen at a frequency where they increasingly overlap, thereby compounding the difficulty of managing them. The survey asked two questions about this situation. The first showed that security professionals do not see this as an increasingly worrisome trend. Most of them said the number of times they had to deal with multiple security incidents at the same time had remained about the same compared to a year ago (56 percent). For a quarter of security professionals, instances of multiple security incidents at the same time had actually decreased (26 percent); it only increased for 18 percent (see Figure 2.7)

However, when multiple security incidents did overlap, there were usually byproducts. Only 15 percent of security professionals said that they had adequately planned and resourced for the overlapping incidents they faced and so they had not experienced any of the byproducts of overlapping security incidents.

Nearly half of respondents said dealing with multiple incidents stretched resources, making the organization potentially vulnerable to new threats (44 percent) or that it caused stress on security staff, potentially leading to decreasing

Figure 2.7: Trend of Overlapping Security Incident Frequency

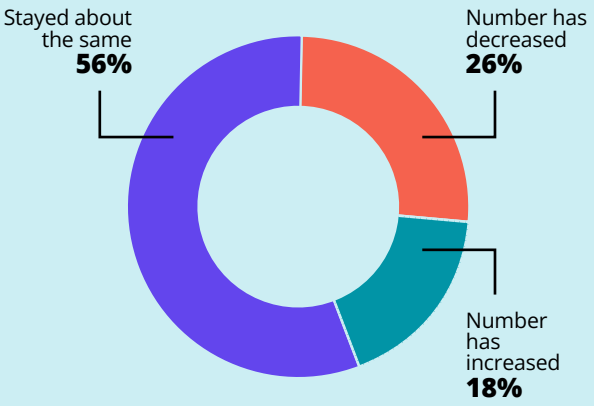
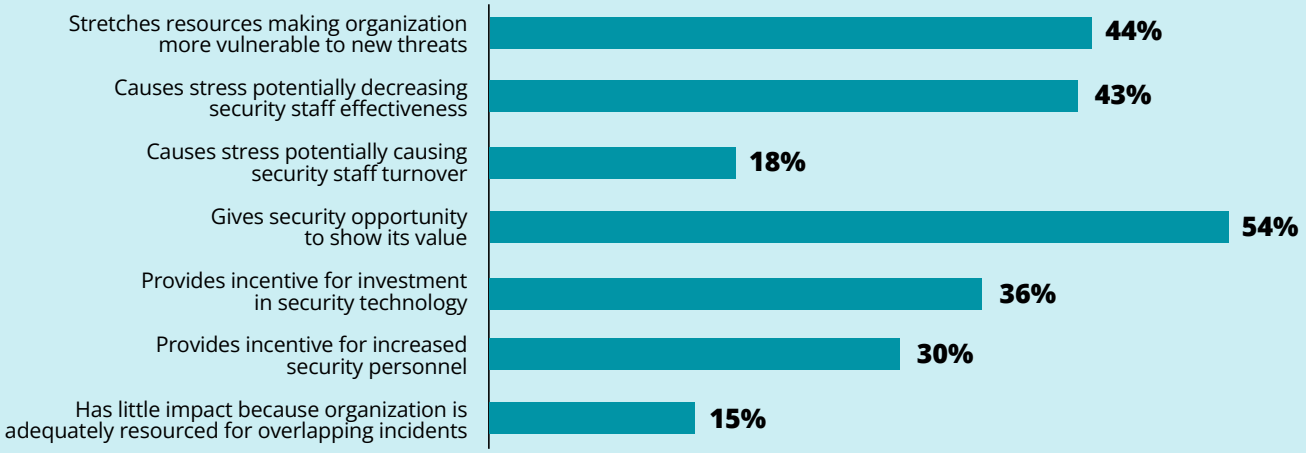


Figure 2.8: Consequences of Overlapping Security Incidents



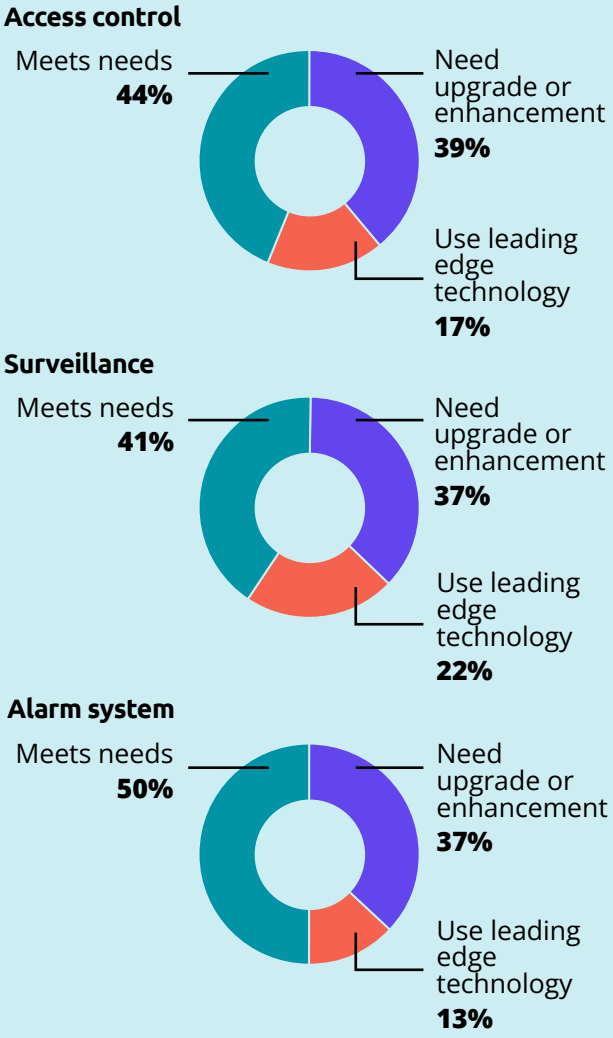
effectiveness (43 percent). Far fewer (18 percent) thought the stress of dealing with multiple incidents might lead to security staff turnover (see Figure 2.8).

Dealing with multiple incidents also could have positive consequences. More than half (54 percent) said such occasions gave security an opportunity to show its value to the organization. Others said it could be used to procure increased investment in security technology (36 percent) or personnel (30 percent).

SECURITY SYSTEMS' ROLE IN INCIDENT PREPARATION, IDENTIFICATION, AND RESPONSE

The research examined three general types of security technology of particular importance to incident management: access controls, surveillance, and alarms. For each, this report provides benchmarks on the current state of these technologies in organizations and examines the impact they have on security incident management.

Figure 3.1: Current State of Security Technology



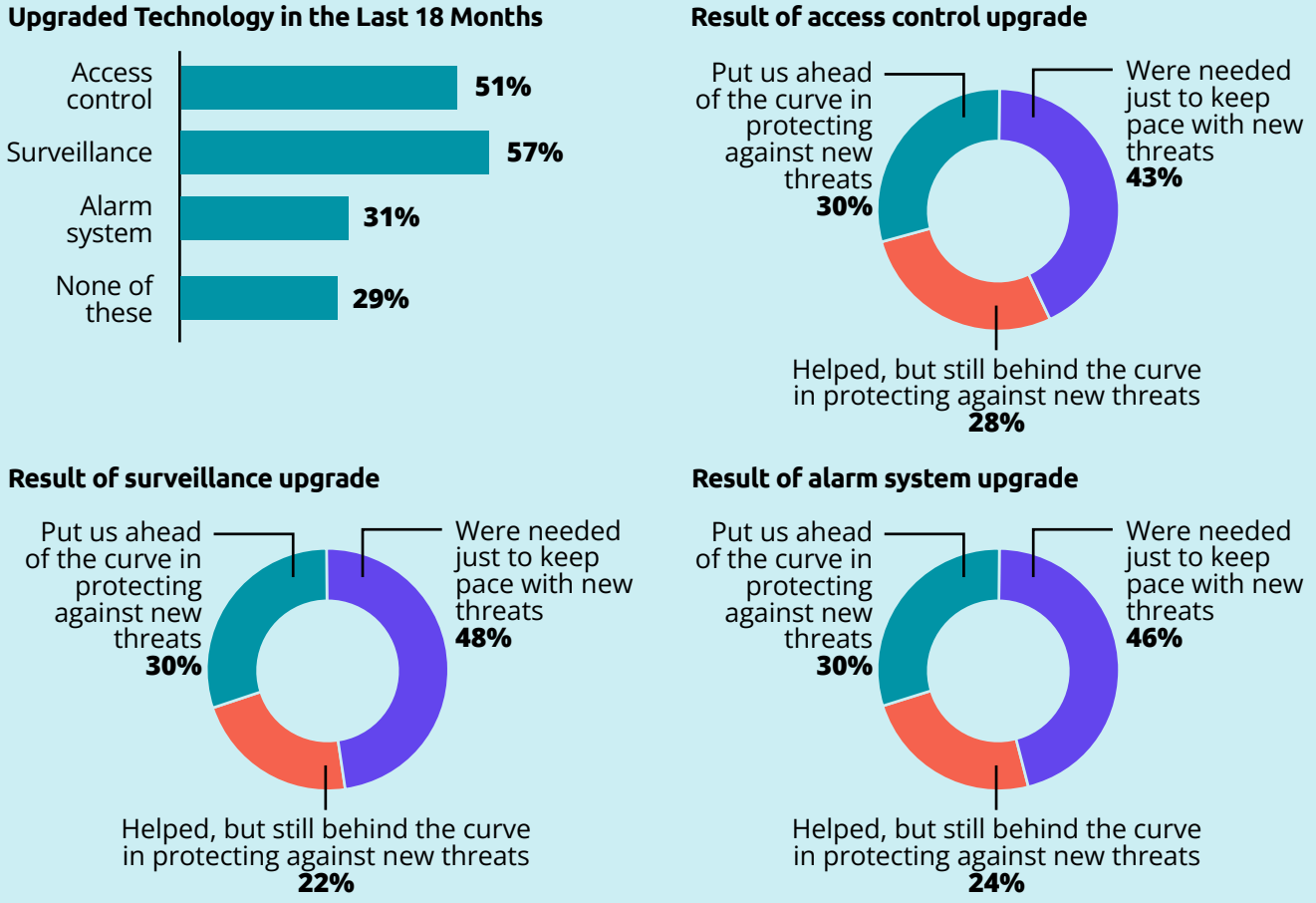
The survey asked if their technology solutions in each area met their needs, was leading edge technology, or if they thought they needed an upgrade or enhancement. Few security professionals said they had deployed leading edge technology, and more than one-third said they needed to upgrade or enhance (see Figure 3.1).

Security professionals were then asked if they had upgraded their access control, surveillance, or alarm systems in the past 18 months. Those that had upgraded then answered questions regarding the impact the new systems had on their ability to deal with the threats they faced.

More than half had upgraded their access control (51 percent) and surveillance (57 percent) systems in the past 18 months, and nearly one-third had upgraded their alarm system (29 percent). However, respondents revealed that most of these upgrades were needed just to keep pace with the emerging threat landscape and did not give security professionals the sense that they had gotten ahead of new and emerging threats. In fact, in nearly one quarter of cases, security professionals said that while the upgrades may have helped some, they still felt behind the curve.

These findings were remarkably consistent no matter which type of security technology was recently upgraded (see Figure 3.2):

Figure 3.2: Utility of Security Technology Upgrades



- Access control: 43 percent said the upgrades enable them to just keep pace with the emerging threat landscape, and 28 percent still felt like more was needed in that area.
- Surveillance: 48 percent said the upgrades enable them to just keep pace with the emerging threat landscape, and 22 percent still felt like more was needed in that area.
- Alarm system: 46 percent said the upgrades enable them to just keep pace with the emerging threat landscape, and 24 percent still felt like more was needed in that area.

In addition, the survey researched the effects the upgrades had on incident management. This data is presented in the Factors that Make Security More Effective at Managing Incidents section.

LEARNING FROM SECURITY INCIDENTS

"Investigations almost always reveal valuable information. Among other things, they might uncover a condition or weakness that allowed a crime to be perpetrated, afforded unauthorized access, created an opportunity for malicious activity, produced inadvertent hazards, or enabled some other anomaly to occur. Findings or results of investigative activity that reveal a condition, policy, practice, or vulnerability that places assets at risk should be documented and addressed."

The preceding statement is from ASIS International's Protection of Assets: Security Management publication and succinctly states why incident after-action reports are so critical for organizations that want to engage in continuous improvement processes. The importance of such reports underscores the research finding that almost all organizations (90 percent) create after-action reports following security incidents (see Figure 4.1). Of those who do, almost all of them—88 percent—say the after-action reports have led to meaningful security changes at their organizations (see Figure 4.2).

Researchers then asked what kinds of changes the reports have led to. Almost three-quarters (73 percent) of respondents said that after-action reports been used in security awareness materials or training. Perhaps most importantly, incident after-action reports are incredibly useful to justify the need to increase investment in security technology or personnel. More than half of respondents (52 percent) said that their reports had led to increased security resources.

Figure 4.1: Does Your Organization Create Incident After-Action Reports?

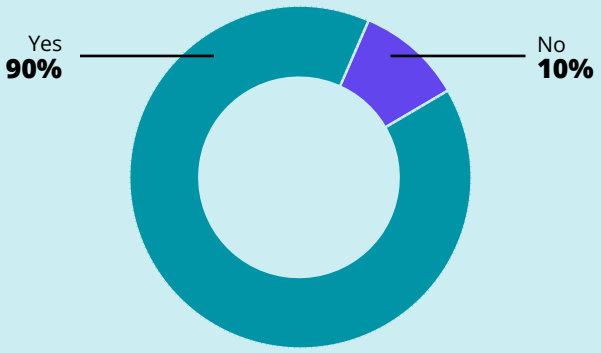
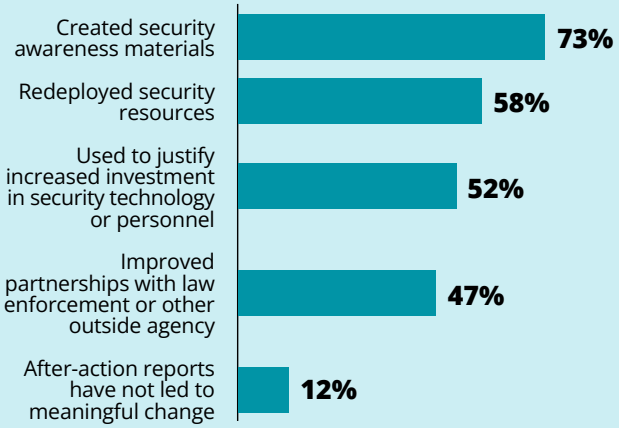


Figure 4.2: Actions Taken as a Result of After-Action Reports

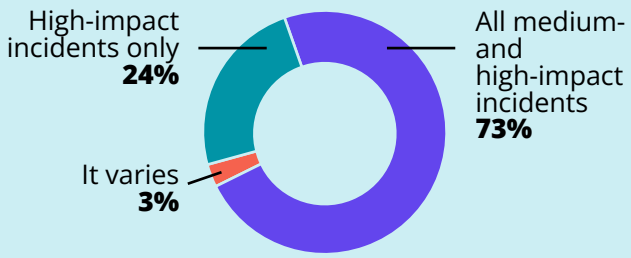


Security professionals also used incident after-action reports to redeploy security resources (58 percent) and to improve partnerships they have with law enforcement or other outside agencies (47 percent). After-action reports also have a significant impact on how effectively organizations handle security incidents. For more details, see the Factors that Make Security More Effective at Managing Incidents section.

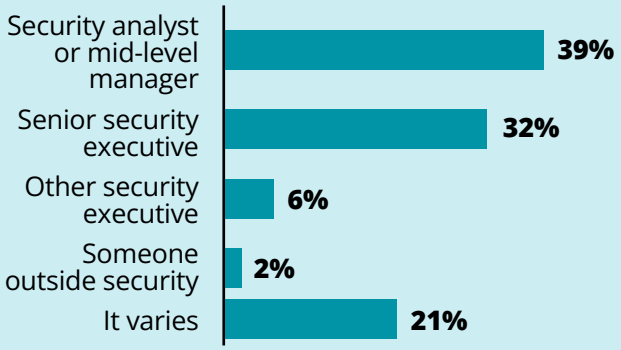
In addition, the research captured several benchmarks related to security incident after-action reports. Figure 4.3 presents findings on the types of incidents that trigger after-action reports, who writes the reports, and how they are presented.

Figure 4.3: Security Incident After-Action Report Benchmarks

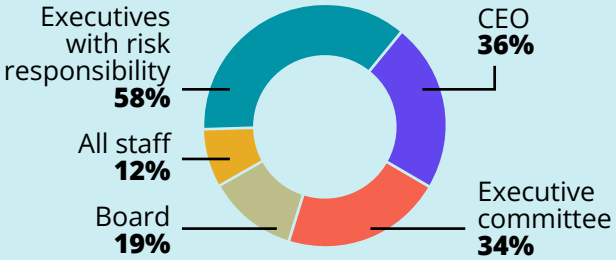
What type of incident triggers an after-action reports



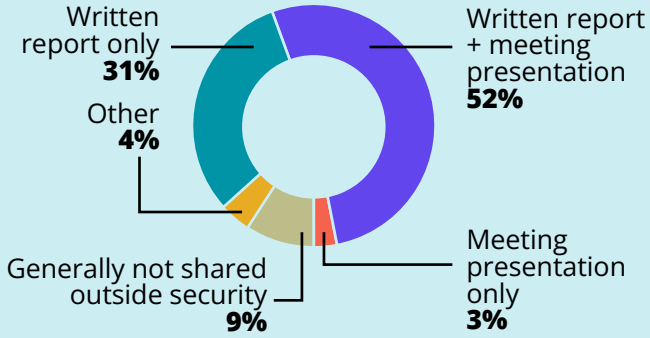
Who writes security incident after-action reports



Who receives security incident after-action reports



How are security incident after-action reports communicated



FACTORS THAT MAKE SECURITY MORE EFFECTIVE AT MANAGING INCIDENTS

How effective is your organization at managing security incidents? It's a difficult and necessarily subjective question.

In some cases, the survey asked the question directly: For the different kinds of technology featured in the survey, researchers asked the direct questions. However, with the survey providing primarily benchmarking data, researchers used a secondary, indirect method of ascertaining effectiveness.

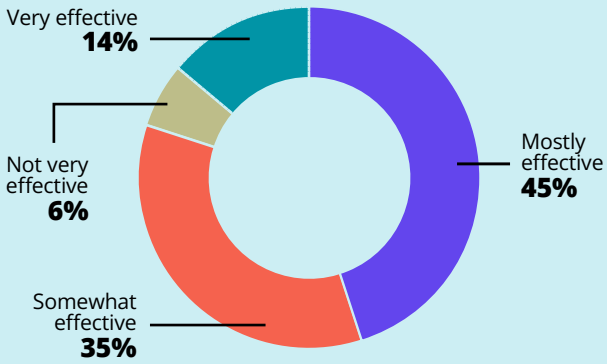
The survey asked the question: Overall, how effective is your organization at managing security incidents? Security professionals were given a five-point scale ranging from 1-Not at all effective (almost no one chose this) to 5-Very effective (14 percent selected this highest rating) to choose from (see Figure 5.1). Researchers then crosstabulated this overall effectiveness question with the benchmarking data to measure how other variables affected the degree to which security professionals thought their security incident management was, overall, effective. This comparison assumes that, when averaged out of more than 400 responses, the security professionals who say their organizations are either very effective or mostly effective do, in fact, work at organizations that are more effective at managing incidents than other organizations.

From the direct questions and the crosstabulations, four critical success factors emerged.

INVESTING IN SECURITY TECHNOLOGY

As noted above, the survey measured the effectiveness of access control, surveillance, and alarm systems with direct questions. Specifically,

Figure 5.1: How Effective Is Your Organization at Managing Security Incidents



any security professional who reported they had upgraded any of those technologies was asked a follow-up question: Did the upgrade result in any of the following benefits:

- Enable quicker or accurate assessment of incident severity
- Enable quicker response to many incidents
- Contributed to significantly fewer incidents
- Kept incidents from escalating
- Enable better post-incident analysis
- Enable redeployment of security personnel to higher impact responsibilities

In addition, participants were given a "None of the above" choice, and it's the examination of this choice that shows upgrading any of the three types of technology—access control,

surveillance, or alarm systems—increases the effectiveness of their organization's security incident management. For access control, 84 percent chose one or more of the above benefits; for surveillance, 97 percent chose one or more of the above benefits; and for alarm systems, 89 percent chose one or more of the above benefits.

It's also notable that the leading benefit for each technology type was enabling a quicker response time (the full dataset for each technology is in Figure 5.2), which reinforces the next success factor.

But first, the overall effectiveness question also supports technology as a critical success factor. One question asked security professionals if their current system in each of those areas was in need of upgrade, mostly met needs, or was leading edge (see Figure 3.1). When compared to the number of professionals who said their organizations were either very or mostly effective overall at incident management, a clear pattern emerged.

In each technology type, if the respondent said they were on the leading edge, they also rated their overall effectiveness at managing security

Figure 5.2: Incident Management Benefits of Technology Upgrades

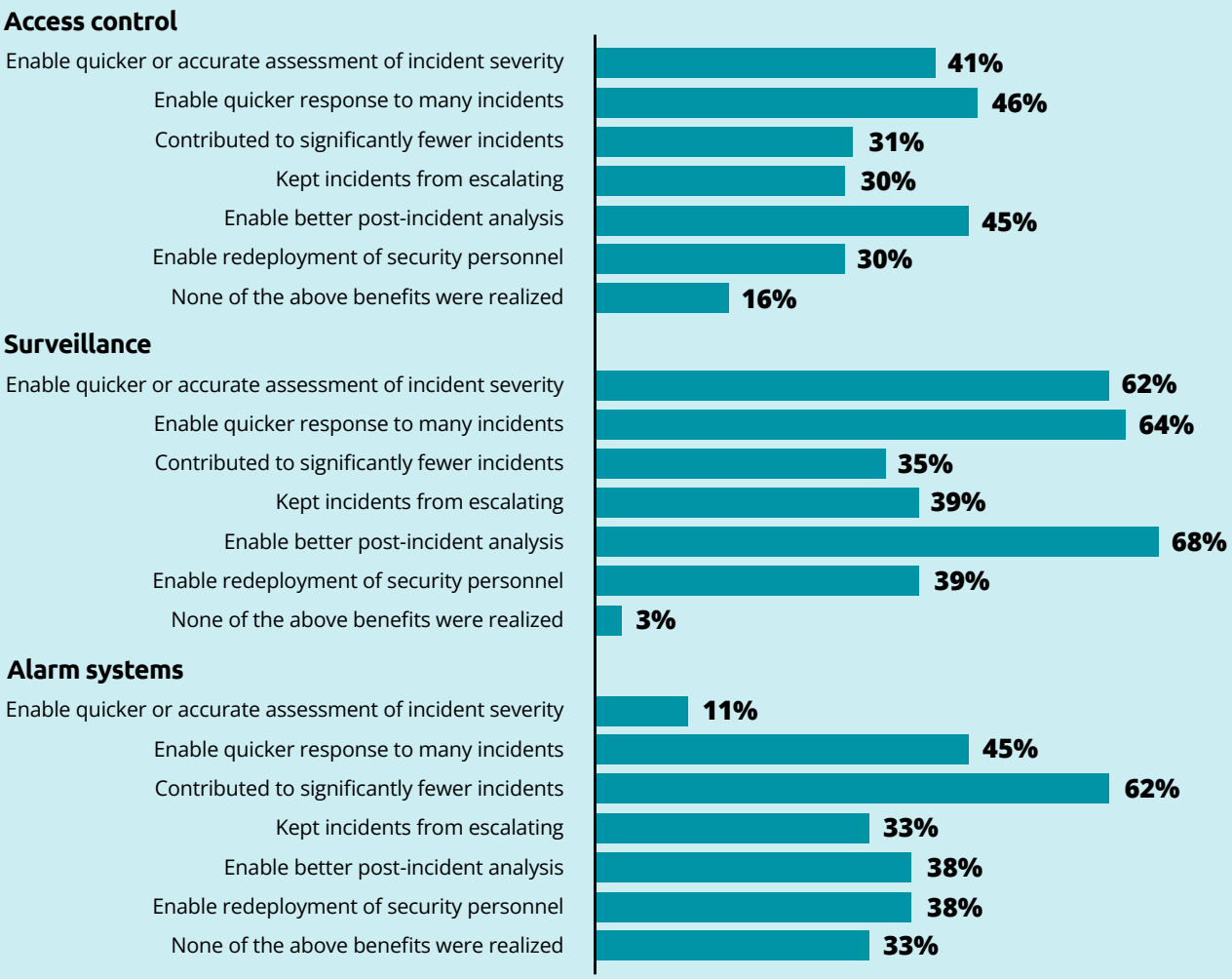


Figure 5.3: Overall Effectiveness Measure by State of Current Technology

incidents as either very or highly effective: from a low of 79 percent for those with leading edge alarm systems to a high of 86 percent for those with leading edge access control technology. Conversely, respondents who said they needed to upgrade their technology were much less confident in their overall effectiveness. In each case, the number who said their organizations were either very or mostly effective at overall security incident management was below 50 percent (see Figure 5.3).

IMPROVING RESPONSE TIME

Being able to detect and respond to security incidents as quickly as possible was perhaps the strongest effectiveness measure in the study. As noted earlier, most security professionals (60 percent) are mostly happy with their detection and response time, but would welcome incremental improvement. However, more than a quarter (28 percent) would like to see significant improvement in this area, and 13 percent said they were very happy with their detection and response time and any further attempts to improve would be unlikely to make significant improvements.

When compared with the effectiveness measure, an overwhelming number of security professionals who said there was little room for improvement in response time also said their organizations were either very or mostly effective at incident management: 93 percent. This compares to only 32 percent of professionals who would like to see significant improvement in response time (see Figure 5.4).

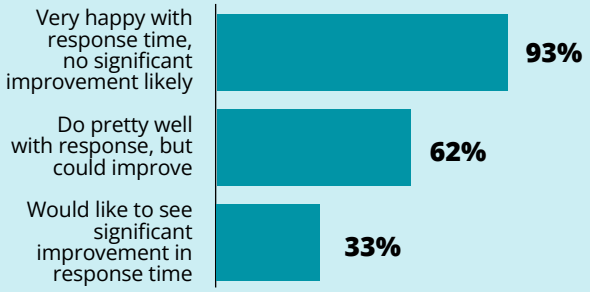
STAFFING A SECURITY OPERATIONS CENTER 24/7

The survey asked respondents to rate the level of impact several different practices and capabilities had on incident prevention and response, again, using a five-point scale with “little or no impact” on one side and “major impact” on the other. Each option scored highly, but having a security operations center (SOC) functioning all the time scored the best with a weighted average of 3.86 (so it fell between having a “medium level of impact” and “significant impact,” but almost all the way toward “significant impact” side). (See Figure 2.4.)

This finding was reinforced with the overall effectiveness question: 59 percent of those with 24/7 SOCs were very or mostly confident in their organization’s overall security incident management

Figure 5.4: Overall Effectiveness Measure of Incident Response Time

Percent who said their organization was very or mostly effective at security incident management



effectiveness. Only 38 percent of those without 24/7 SOCs were as confident (see Figure 5.5).

USING INCIDENT AFTER-ACTION REPORTS

Both the process of creating after-action reports and actually putting them to use contributed to the confidence security professionals have that their organizations effectively manage incidents.

Of the 88 percent of organizations that create after-action reports, 64 percent of security professionals say their organizations are very or mostly effective at incident management. That percentage tumbles to 36 percent for the 12 percent that do not create after-action reports (see Figure 5.6).

Actually using the reports to effect change was also a sign of effective incident management, though the corroboration is not as strong. The previous section described various actions the reports may have precipitated, such as improving relations with law enforcement or using them to create security awareness tools. No matter which action the organization took, it led to a higher effectiveness rating than organizations where after-action reports did not lead to any meaningful change (see Figure 5.7).

Figure 5.5: Overall Effectiveness Measure of 24/7 SOC

Percent who said their organization was very or mostly effective at security incident management

Figure 5.6: Overall Effectiveness Measure of Creating Incident After-Action Reports

Percent who said their organization was very or mostly effective at security incident management

METHODOLOGY

This research project commenced in September 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, VOLT. The volunteer group shaped the survey questionnaire, which was deployed in late September 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 618 people answered at least some of the questions, and 433 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 ±5 percent at the 95 percent confidence level.

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	28%
Variety of facility types in multiple regions or locations, primarily within single country	29%
Multiple facilities primarily in a single region	25%
Mostly a single facility or single campus with a few facilities	18%
Region	
North America	39%
Central America, South America, Caribbean	7%
Europe	9%
Middle East	6%
Africa	15%
Oceania	1%
Asia	16%
Multiple regions	8%

Number of Employees (or Employees and Students)	
1 to 100	17%
101 to 1,000	24%
1,001 to 10,000	29%
10,001 to 50,000	17%
50,001 to 100,000	6%
More than 100,000	8%
Industry	
Amusement, gambling, or recreation	1%
Banking, finance, insurance	7%
Consulting and professional services	6%
Defense and intelligence	5%
Education, K-12	1%
Education, university	3%
Emergency Services	1%
Food and agriculture	2%
Healthcare	4%
Hospitality and food services	3%
IT and telecommunications	4%
Law enforcement	3%
Manufacturing	8%
Media and entertainment	1%

Museums and cultural properties	2%
Oil, gas, chemical	8%
Pharmaceutical	3%
Public administration/government (nondefense, law enforcement, or education)	3%
Real estate and construction	2%
Retail	2%
Security services	17%
Transportation and supply chain	5%
Utilities	2%

Title	
CSO or VP of security	13%
CISO	1%
Other c-suite executive	2%
Director of security	16%
Other director (facilities, risk, compliance, etc.)	2%
Senior manager of security	18%
Manager of security	27%
Other manager (facilities, risk, compliance, etc.)	3%
Frontline security	5%
Security consultant or business partner	6%