Threat Intelligence

Understanding How Threat Management Supports Resilient Organizations

ASIS INTERNATIONAL | SECURITY ISSUES RESEARCH

Sponsored by

esri

Contents

ASIS INTERNATIONAL
Advancing Security Worldwide®

ASIS International thanks Esri for their sponsorship of this research. www.esri.com

esri

Definitions

threat: Potential cause of an unwanted incident, which may result in harm to individuals, assets, a system or organization, the environment, or the community.
Source: ASIS Security Risk Assessment Standard

threat analysis: Process of identifying and quantifying the potential cause of an unwanted event, which may result in harm to individuals, assets, a system or organization, the environment, or the community.
Source: ASIS Security Risk Assessment Standard

threat information: Any information related to a threat that might help an organization protect itself against the threat or detect the activities of an actor.
Source: NIST SP 800-150

threat intelligence: Threat information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision-making processes.
Source: NIST SP 800-150

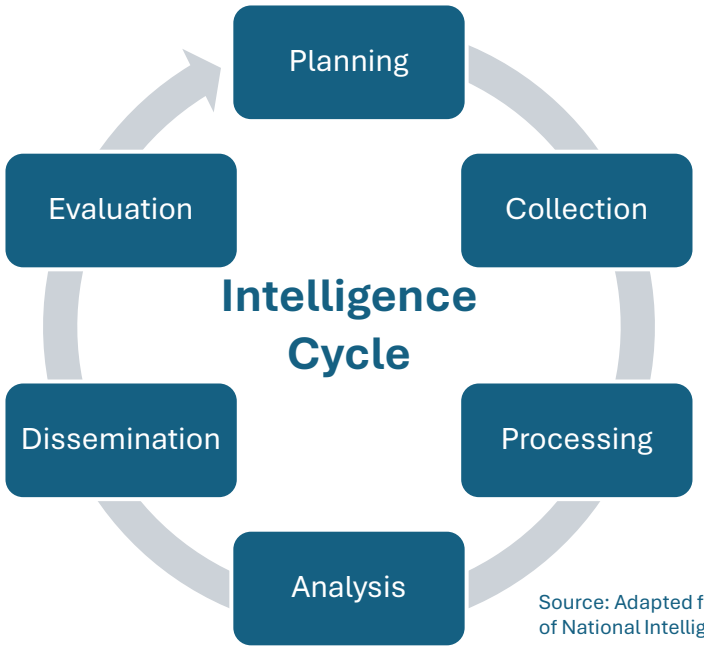
resilience: Adaptive capacity of an organization in a complex and changing environment.
Source: ASIS Security Risk Assessment Standard; ISO Guide 73:2009

Introduction

The speed of business is a cliché for a reason. The ability to take quick, decisive action is a business differentiator.

The areas of threat management, risk management, crisis management, and business continuity contribute to an organization's resilience capacity. The threat intelligence component of threat management is one of the main ways velocity enters the organizational resilience equation. The quicker an organization can identify, analyze, and interpret information about potential threats, the quicker it can make plans to neutralize, avoid, or otherwise mitigate the threat. This makes threat intelligence—which is typically a security function—a preeminent way security can act as a key business differentiator in the organization.

The *Threat Intelligence: How Threat Management Supports Resilient Organizations* report studies the types of threats organizations scan for, what they use to identify threats, how well they perform at threat identification, how effective they are at the intelligence cycle, and the impact threat intelligence has on resilient business functions.



Source: Adapted from U.S. Office of the Director of National Intelligence

Key Findings and Conclusions

The survey provided threat intelligence benchmarks and insights that relate to every phase of the intelligence cycle.

Planning

Unsurprisingly, security plays a seminal role in threat intelligence and how it is collected and used in an organization. (Page 6)

Threat intelligence is important to a variety of important business functions, including business continuity, emergency or crisis management, enterprise risk management, and organizational resilience. (Page 14)

Collection

Organizations use a variety of methods to collect threat intelligence, with open-source intelligence leading the way. Which method is deemed most important? That's information from governmental or cooperative partnerships. (Page 11)

Organizations are best at gathering intelligence on physical security incidents and political or civil unrest. They are worst at gathering intelligence on climate change, supply chain disruptions, and national or international crime trends. (Page 7)

Processing

Major robberies or burglaries, workplace violence incidents, and physical perimeter breaches were the hardest types of incidents to detect in a timely fashion; regulations or standards changes, political instability, and civil or political unrest were the easiest. (Page 9)

Geospatial intelligence gives significant advantages to those who use it in threat management. This is particularly true in the effectiveness of gathering meaningful information and improving the speed of the entire threat intelligence cycle. (Page 13)

Analysis

Security professionals rated their organizations' effectiveness highly across all threat intelligence processes, including "analyzing/prioritizing threat intelligence." Security consultants agreed, scoring the effectiveness of organizations in analyzing and prioritizing threat intelligence higher than other processes. (Pages 6 and 17)

Dissemination

Security professionals rated their ability to communicate intelligence to business units higher than any other threat intelligence process, with 35 percent saying their organization was extremely effective at it. (Page 6)

Despite that rating, it was also one of the areas most likely to have broken down when organizations experienced an incident that caused a serious business disruption. Incidents involving regulations or standards changing fared the worst in this area, followed by economic instability, cybercrime, and civil or political unrest. (Page 9)

See the next page for key findings and conclusions related to the **Evaluation** phase of the intelligence cycle.

Key Findings and Conclusions: Evaluation

The research asked security professionals to rate the effectiveness and contributions of various aspects of threat intelligence, as well as assessing the role threat intelligence plays in key organizational resilience functions.

Evaluation

Security professionals were generally highly upbeat about their organizations' ability in each part of the threat intelligence cycle—giving high marks in gathering intelligence, analyzing it, making decisions, and communication. When asked to rate the speed of the process as whole, the ratings fell significantly. This highlights a potential opportunity to look for ways to be more efficient. (Page 6)

Of the 12 types of incidents asked about in the survey, incidents involving economic instability, political instability, and regulation or standards changes proved the most difficult to identify, respond to, and recover from. Organizations fared better when faced with incidents related to labor unrest, civil or political unrest, or workplace violence. (Page 8)

Of those who experienced a serious business disruption recently, almost two-thirds report that they expect their organization to handle a similar incident much better in the future—just 6 percent say they do not think their organizations made changes that will have a positive impact. (Page 10)

Such serious, disruptive incidents led organizations to make changes in two areas: (1) threat intelligence communication processes and (2) emergency management or business continuity processes. Fewer said they made changes to how threat intelligence is analyzed or made investments in new threat intelligence technology. (Page 10)

When looking at various resilience-related business functions, security professionals reported that threat intelligence had the biggest impact on crisis management, while the other functions—business continuity, enterprise risk management, and overall organizational resilience—also rated highly. (Page 14)

In terms of how threat management is structured, having a centralized approach to threat intelligence and having security lead or play or major role in threat management has a substantial impact on how effective organizations are in all of the resilience-related business functions. (Page 15)

Characteristics of Threat Intelligence

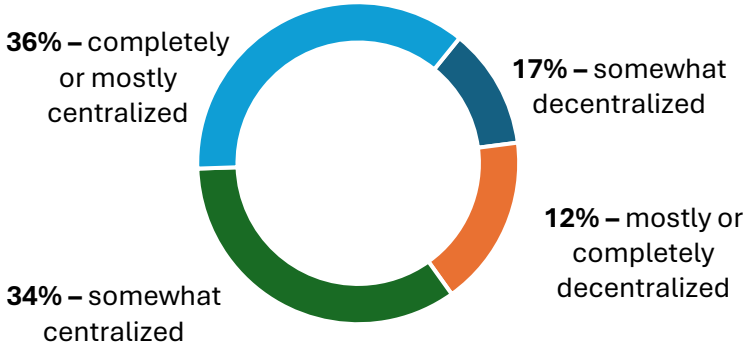
Having a centralized organizational approach to threat intelligence management signifies a mature approach to threat management and helps make the intelligence cycle efficient and effective.

Overall, survey participants reported their threat intelligence function was more centralized than decentralized.

In most cases, security either manages the threat intelligence or plays a major role. In just about every organization, security plays some role. This is important because effective threat intelligence is an important way security can provide value to the organization.

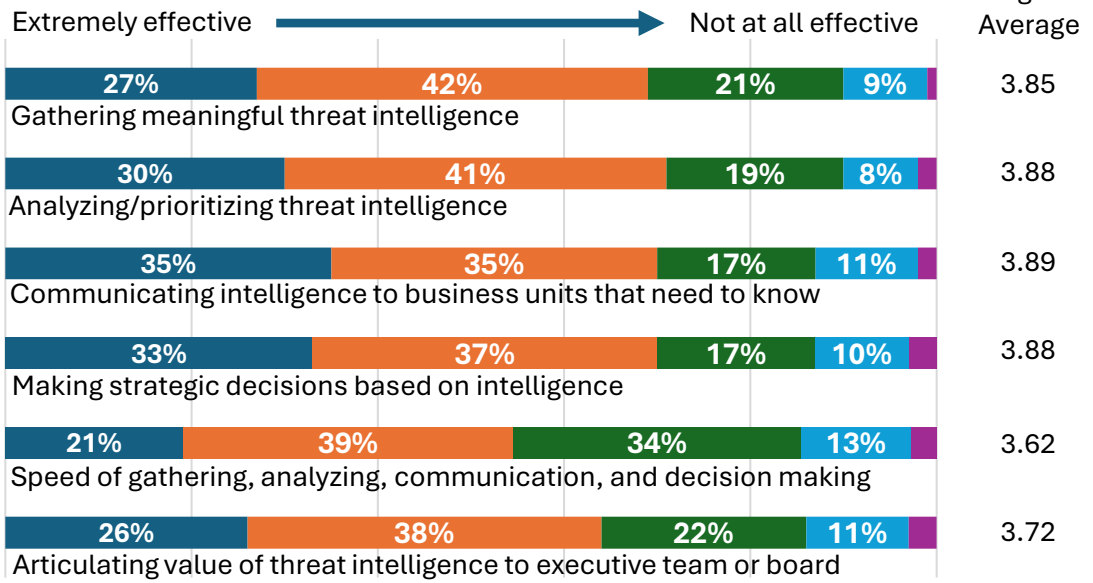
Security professionals were also upbeat about the effectiveness of different threat intelligence processes, with every process rated either extremely or mostly effective by at least 60 percent or respondents.

Threat intelligence is...



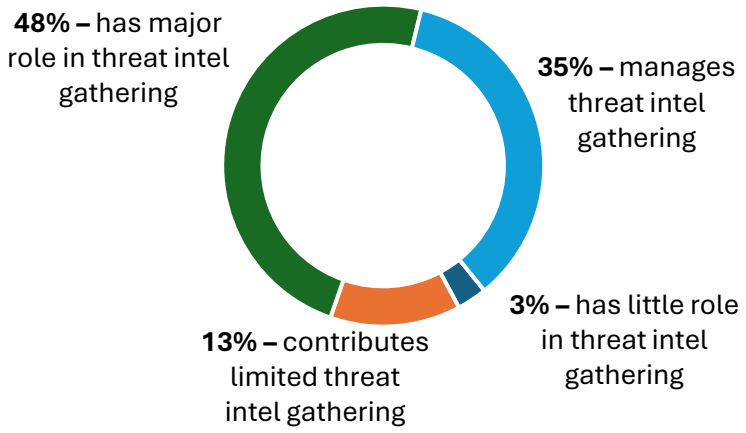
70% completely, mostly, or somewhat centralized

Intelligence Process Effectiveness



(Note: All "not at all effective" ratings were 3% or less.)

Security...



83% manages or has major role in threat intelligence gathering

Percent who said good intelligence on the type of threat was extremely or highly important	
1. Physical security incidents	88%
2. Civil or political unrest	78%
3. Cybercrime	77%
4. Natural disaster	72%
5. Local or regional crime trends	71%
6. Infrastructure stability	70%
7. Regulations or standards changes	69%
8. Political stability	65%
9. Supply chain disruption	64%
10. Economic stability	59%
11. Labor unrest	58%
12. National or international crime trends	56%
13. Climate change	42%

Percent who said their organization was extremely or highly effective at gathering threat intelligence on the type of threat	
1. Physical security incidents	81%
2. Civil or political unrest	71%
3. Cybercrime	65%
4. Local or regional crime trends	64%
5. Infrastructure stability	60%
6. Political stability	60%
7. Regulations or standards changes	59%
8. Natural disaster	58%
9. Economic stability	54%
10. Labor unrest	54%
11. Supply chain disruption	51%
12. National or international crime trends	51%
13. Climate change	32%

Threat Intelligence by Types of Threats

The survey asked participants to rank both how important good intelligence is for 13 different kinds of threats and how effective their organizations were at collecting threat intelligence in that area.

In almost all cases, more than half of respondents said threat intelligence in the area was either extremely or highly important, and more than half reported that their organizations were effective at gathering that intelligence.

The outlier is climate change, where 42 percent rated it as important and only a third said their organization was effective at gathering threat intelligence in the area.

Incidents that Caused Business Disruptions

What kinds of incidents did companies experience? Survey participants were asked if they had experienced an incident that caused significant business disruption in the previous 18 months. One in five (21 percent) had not experienced a major incident in any of the areas.

Top five types of serious incidents

1. Civil or political unrest
2. Natural disaster
3. Physical security breach
4. Supply chain disruptions
5. Regulation or standards changes

Perhaps more importantly, how effectively did organizations identify, respond to, and recover from the incidents that caused major disruptions? (See graph at right.)

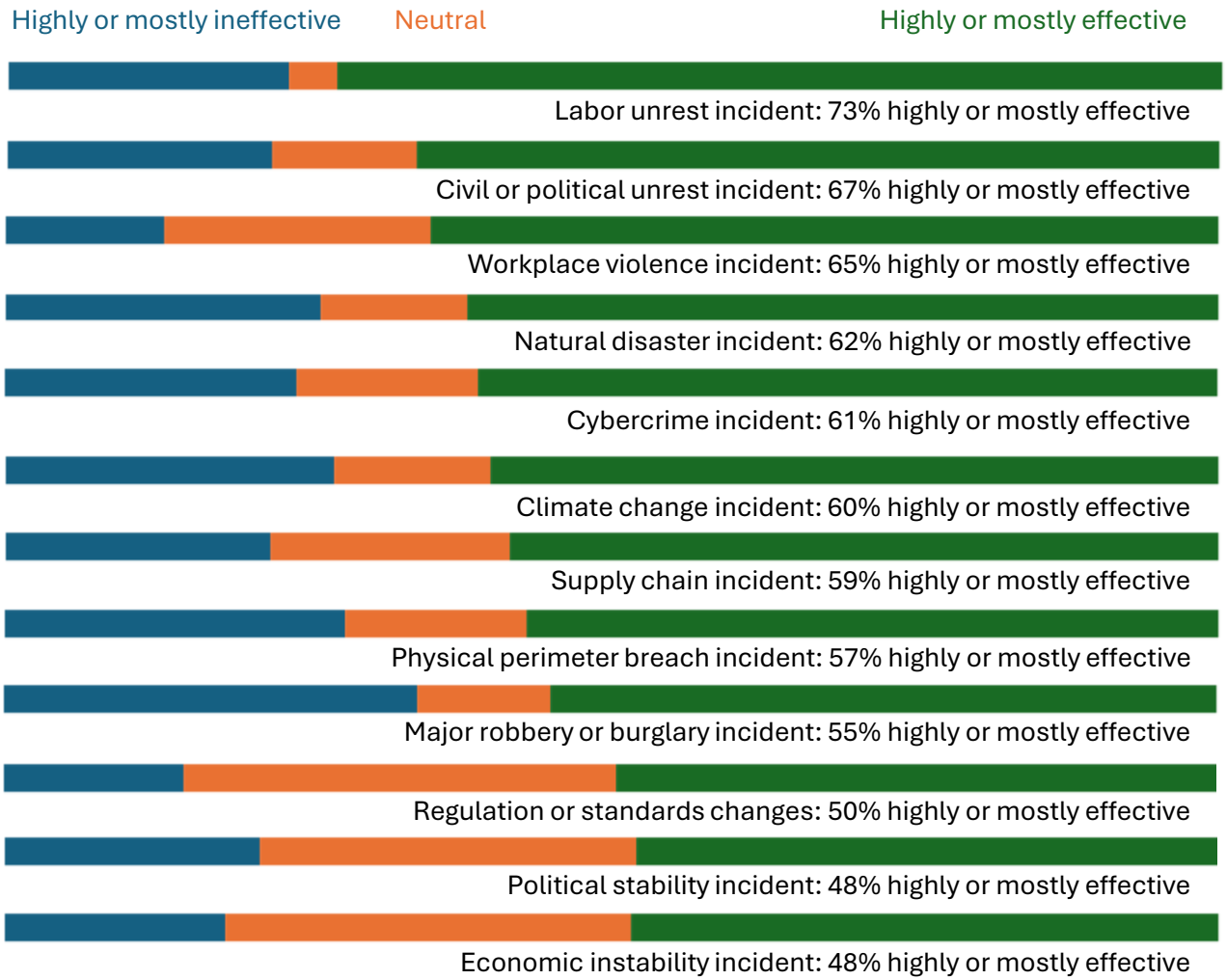
Most effective

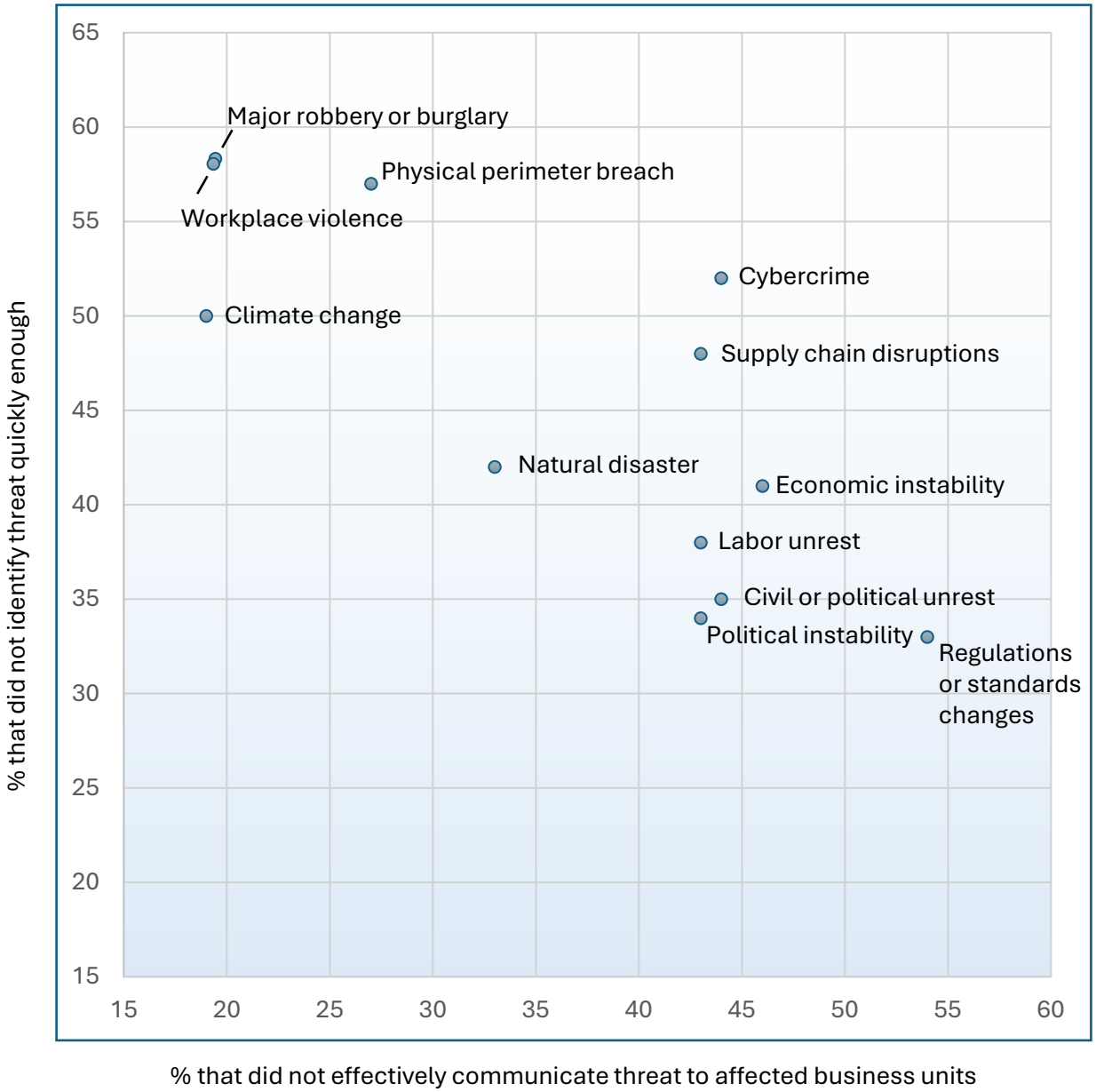
1. Labor unrest incidents
2. Civil or political unrest incidents
3. Workplace violence incidents

Least effective

1. Economic stability incidents
2. Political stability incidents
3. Regulation or standards change incidents

How Effectively Did Organizations Identify, Respond to, and Recover from Incidents that Caused Business Disruption?





Finding the Breakdowns

Post-incident analysis is a critical tool in security. For those who experienced an incident that caused a significant business disruption, the survey asked where the breakdowns occurred. "Not identifying the threat quickly enough" and "not effectively communicating about the threat" had more breakdowns than "failures in emergency management or business continuity." The scatterplot at left shows how often breakdowns occurred in quick identification (vertical axis) and communication (horizontal axis).

Overall, breakdowns occurred in the timeliness of threat identification more often than the other areas, but that was not true for all types of incidents. When the incident was related to changes in regulations or standards, for example, about a third said they did not identify the issue soon enough, while 54 percent said the change was not communicated to business units effectively.

The toughest threats to identify quickly were a major robbery or burglary, workplace violence, physical perimeter breach, and cybercrime.

Breakdowns in emergency management or business continuity processes were less frequent. For every type of incident in the survey, between 22 and 35 percent said a breakdown in this area made the incident worse. The two exceptions: 42 percent for climate change incidents and 19 percent for economic instability incidents.

Achieving Better Outcomes

Whenever an incident causes a significant business disruption, the organization should consider conducing a formal after-action review. The U.S. Army has a simple approach to after-action reviews, one that stands as the basis for the way many approach the practice. The person conducting the review leads discussions with all involved in the events that led to the disruption, working to answer these four questions:

- What was supposed to occur?
- What did occur?
- What went right and what went wrong?
- What should be done differently next time?

A *Harvard Business Review* article expanded on this rubric, giving ideas to ensure after-action reviews lead to meaningful change:

Influence a community not a process. Make your focus the team, the customers, and other members of a community. Identify their motives for wanting change. Uncover the stories of how the event affected them personally.

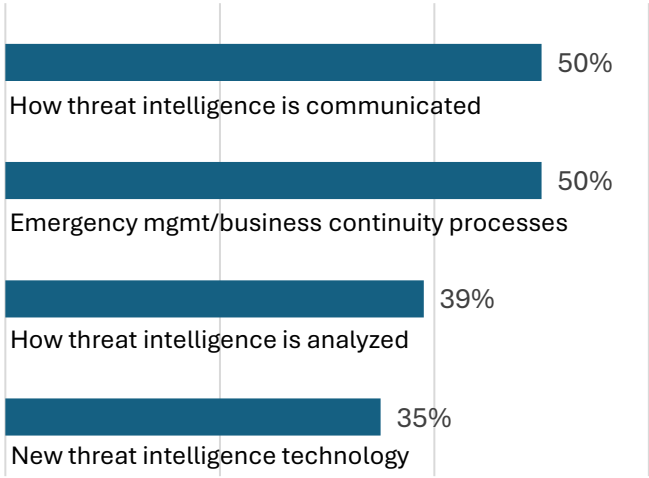
Spend most of your effort on describing what occurred. The authors found most organizations emphasized the last two questions, and as a result pertinent information never surfaced and outcomes tended to support the review leader's preconceived notions of the incident.

Tell the whole story. Most reviews stressed candor by strenuously avoiding assigning blame. The authors said this was a singular source of after-action review failure. Rather than invite actual candor and uncovering the whole story, it tended to shut down investigative avenues when someone accepted responsibility for a shortcoming. Instead, whenever anyone expresses culpability, investigate it thoroughly—review leaders will gain a fuller picture as a result.

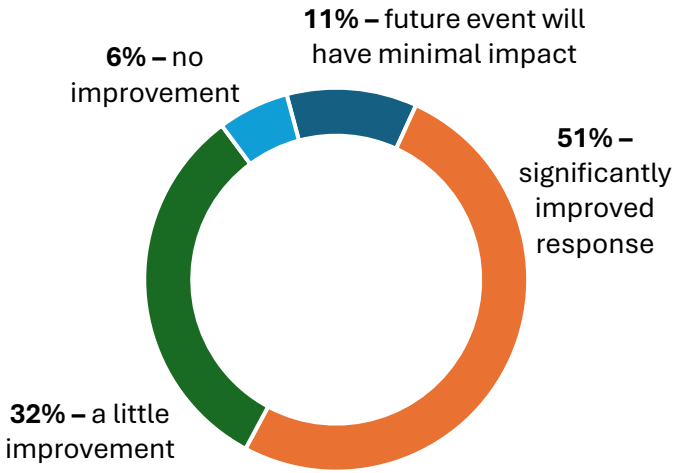
The survey asked participants who reported business disruption incidents what changes they made as a result of the incident and whether or not their organizations would perform better if faced with a similar incident again. Four in five reported making changes in the intelligence cycle, with changes to how threats are communicated to other business units and changes to emergency management or business continuity processes leading the way. Nearly all security professionals said their organization's response to a similar incident would likely improve.

Source: "A Better Approach to After-Action Reviews," Harvard Business Review, 12 January 2023

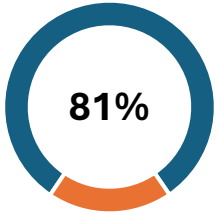
Changes Made as Result of Disruptive Incident



Improved Response for Future Similar Incident

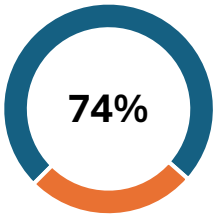


Open-Source Intelligence



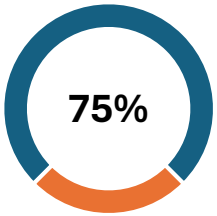
81% of organizations use open-source intelligence; 80% say it is extremely or highly important to threat intelligence.

Security Incident Logs



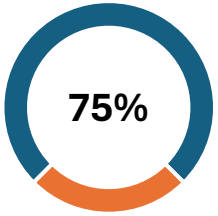
74% of organizations use security incident logs; 86% say it is extremely or highly important to threat intelligence.

Government Sources and Cooperative Partnerships



75% of organizations use government sources and cooperative partnerships; 88% say it is extremely or highly important to threat intelligence.

Direct Observation



75% of organizations use direct observation; 87% say it is extremely or highly important to threat intelligence.

Methods Used to Gather Threat Intelligence

Several methods studied were in place in the vast majority of organizations, and each method was given very high marks for being important to threat identification and management efforts. In fact, the importance ranking was a five-point scale, but the lowest rating of “not at all important” only registered two selections total, one for open-source and one for direct observation—which was far below a 1 percent threshold needed to be charted.

The survey also asked security professionals if each of these threat intelligence methods made threat management presentations to executives or the board more effective. Again, each type scored very highly, however, there was some separation. Fifty-six percent said open-source intelligence made a big difference, and another 36 percent said it helped at least some. The other three methods—security incident logs, government sources and cooperative partnerships, and direct observation—were rated as a big difference maker by between 66 percent and 68 percent of security professionals and somewhat helpful by 26 percent to 29 percent.

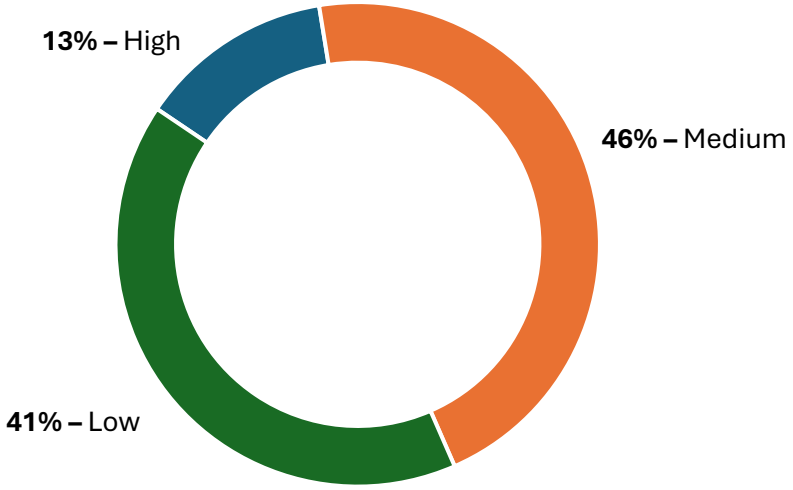
Threat Management Opportunity: Geospatial Intelligence

In addition to the methods on the previous page, the survey asked about one additional method: Geospatial intelligence. (Disclosure: Esri is a sponsor of this report and offers a geospatial intelligence product.) Compared to the other methods, such as open-source intelligence and direct observation, geospatial intelligence is highly specific. Unsurprisingly, fewer survey participants reported using geospatial intelligence in their threat management efforts: 40 percent overall.

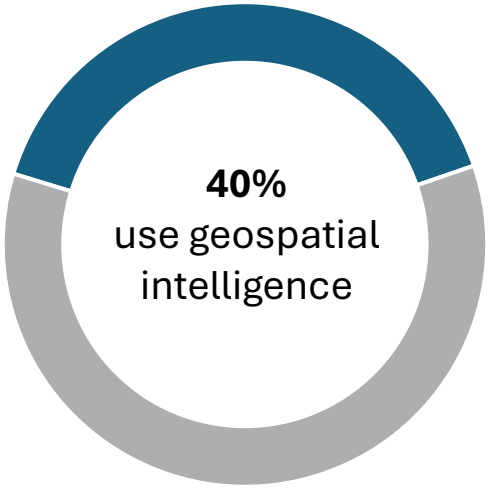
The survey asked the remaining 60 percent why they do not use the technology. No single answer dominated, and when asked to rate their knowledge of the geospatial intelligence, 87 percent said their knowledge was either "low" or "medium," leaving just 13 percent with a high level of knowledge on the topic.

As the next page demonstrates, this presents an excellent opportunity for a lot of organizations to improve their outcomes.

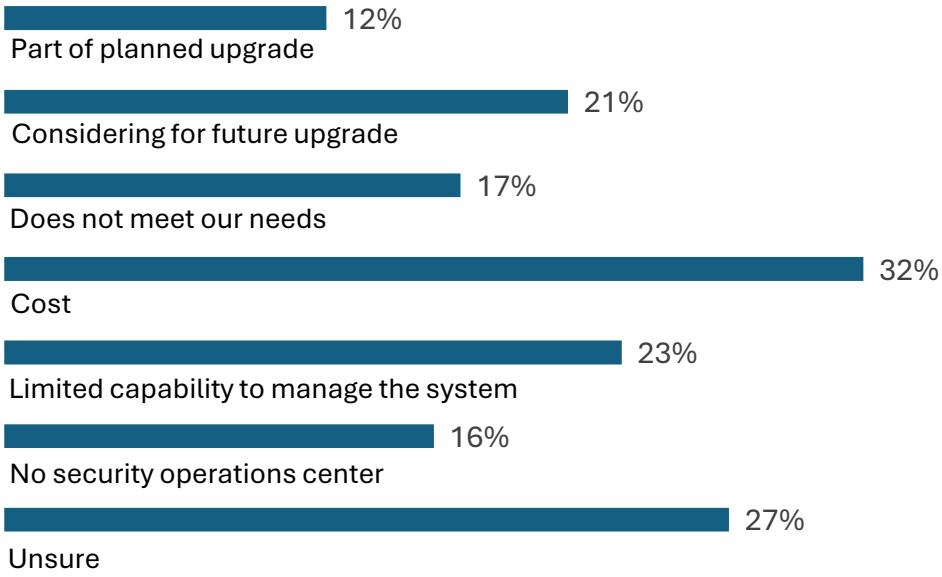
Knowledge of Geospatial Intelligence



Geospatial Intelligence in Threat Management

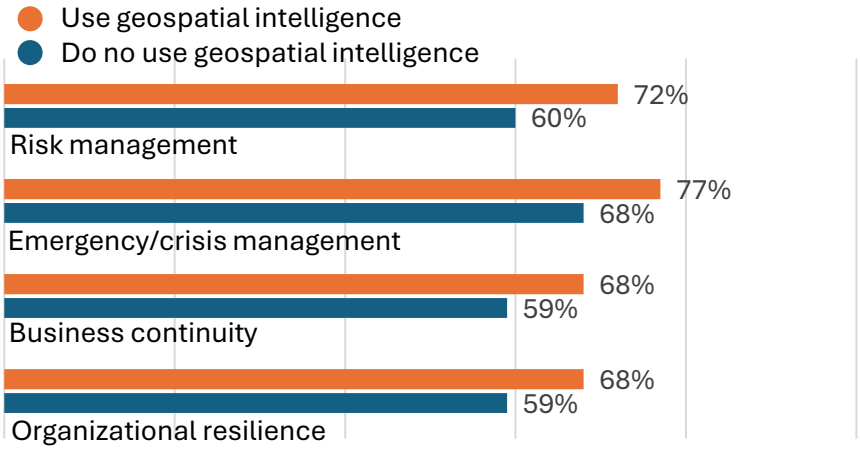


Reasons for Not Using



Mostly or Extremely Effective at Intelligence Functions

Mostly or Extremely Effective at Business Areas



Using Geospatial Intelligence Improves Outcomes

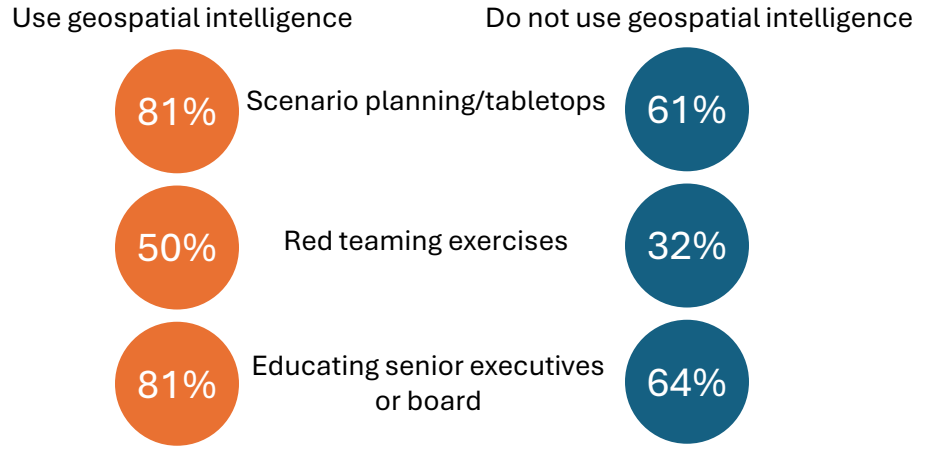
From gathering meaningful threat intelligence to communicating about threats, the security professionals who use geospatial intelligence say they are more effective at threat management processes than those who do not.

The charts at left shows how the 40 percent of respondents who use geospatial intelligence compare in certain areas to the 60 percent who do not. Looking at the starkest example, 80 percent of respondents who use geospatial intelligence say their organizations are mostly or extremely effective at gathering meaningful intelligence overall. That compares to 61 percent for respondents who do not use geospatial intelligence.

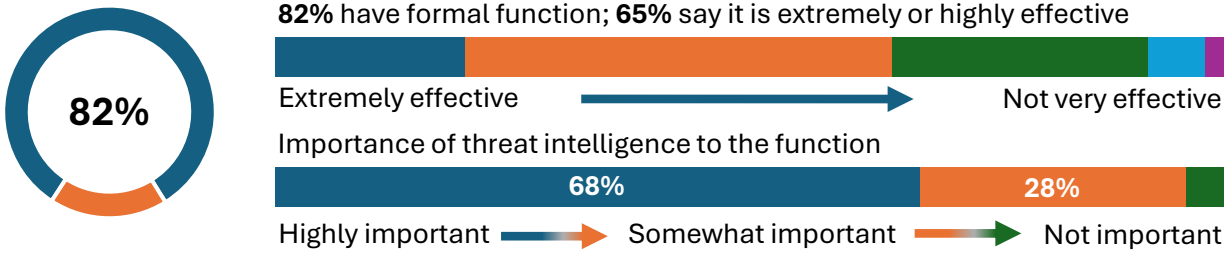
In addition to the threat management process, geospatial intelligence use was related to other positive areas. The survey asked participants to rate their organizations' effectiveness in other business functions, from risk management to organizational resilience. In every case, the 40 percent with geospatial threat intelligence capabilities had higher ratings than the 60 percent without it.

Finally, geospatial intelligence also contributes to other core security resilience functions.

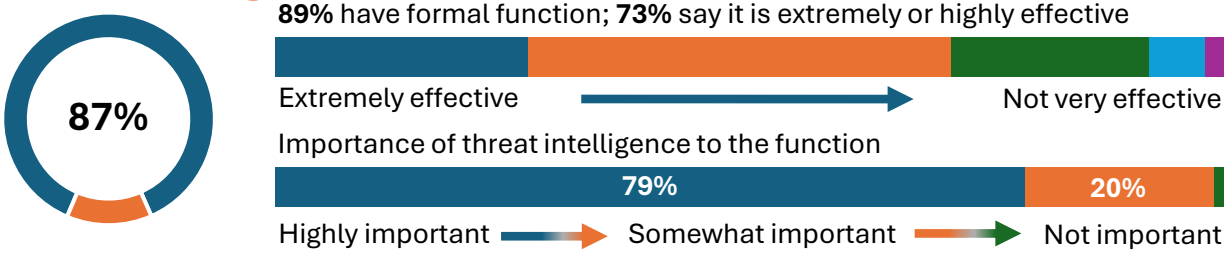
Percent Who Say Threat Intelligence Makes Meaningful Contributions in These Areas



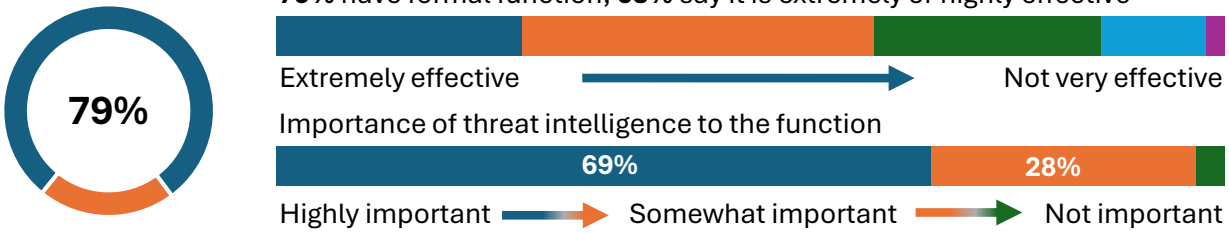
Business Continuity



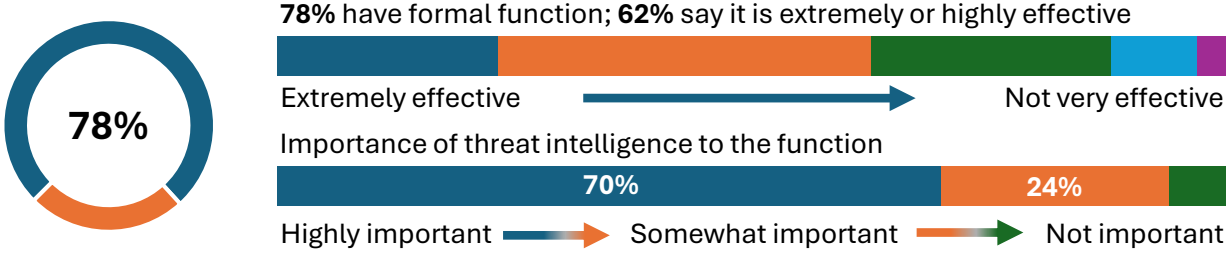
Crisis Management



Enterprise Risk Management



Organizational Resilience



Organizational Resilience Functions and Threat Intelligence

An overwhelming majority of security professionals reported that their organizations had formalized organizational resilience and related functions. How effectively those functions operated varied, however. Overall, security professionals gave their organizations high marks in each of the areas, but crisis management, with 73 percent saying the function was extremely or highly effective, led the way. Just under two-thirds said each of the other functions was extremely or highly effective.

Likewise, security professionals said threat intelligence played an important role in each function, again with crisis management leading the way with 79 percent saying threat intelligence was highly important to the function.

The previous page showed that use of geospatial intelligence made a positive difference in how effective organizations were in each of these areas according to security professionals. The following page takes another look at these areas based on how organizations approach threat intelligence.

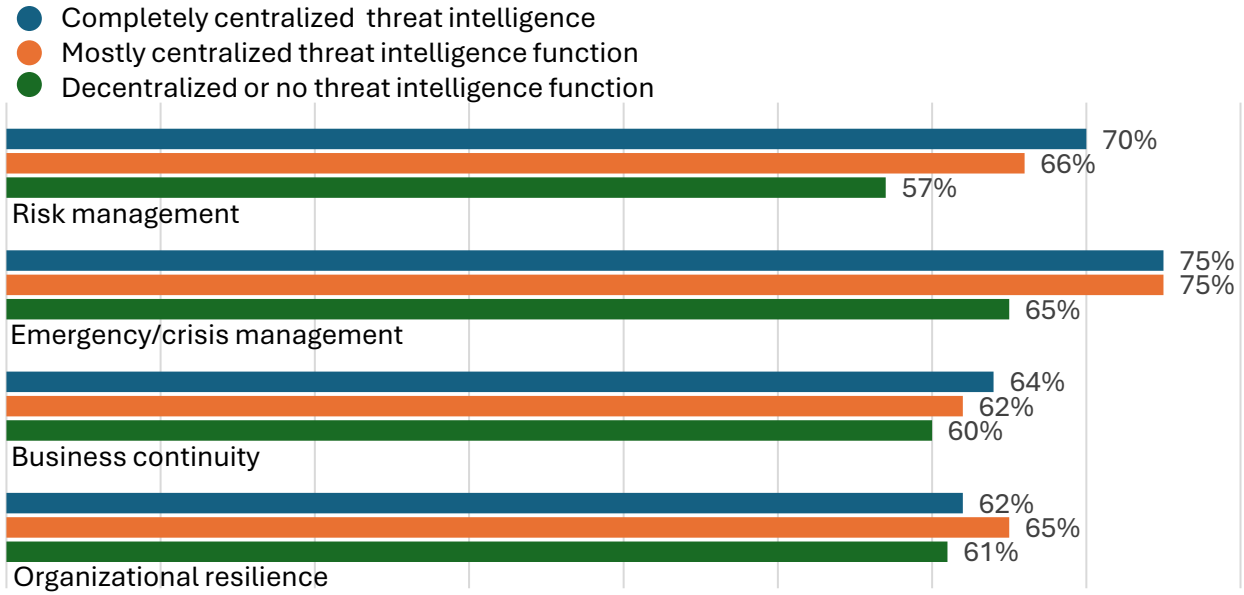
How Security's Threat Management Role Affects Business Areas

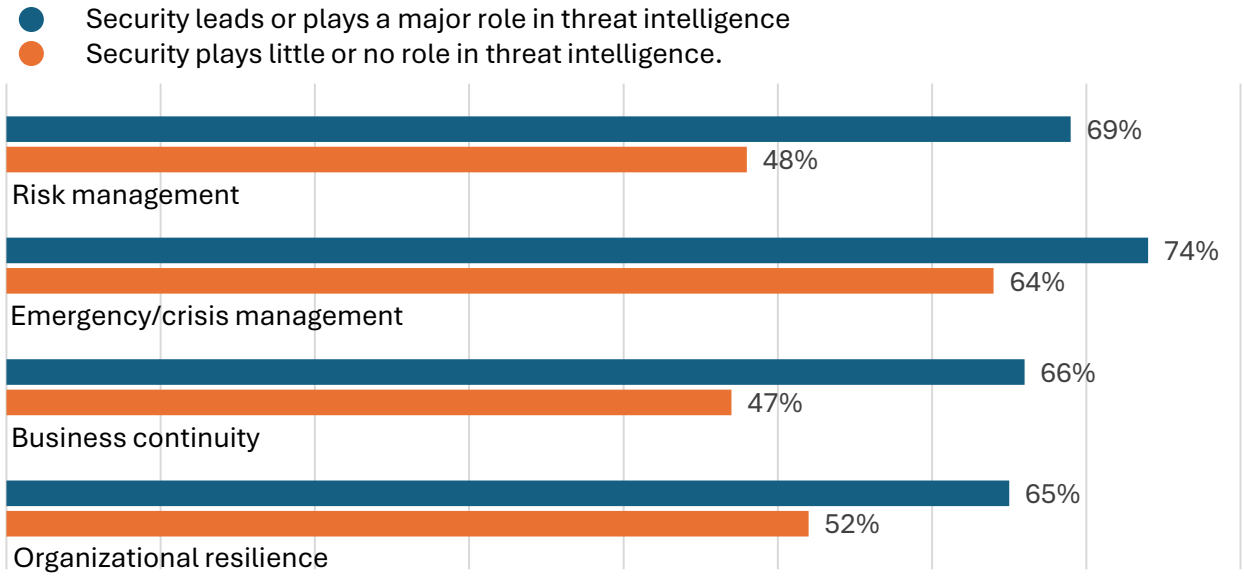
This analysis compares how security professionals rated the effectiveness of resilience-related functions, including overall organizational resilience, with security's role in threat management. The conclusion: organizations should seek to centralize threat intelligence and ensure security plays a major role in threat intelligence processes.

Respondents who said their organizations took a centralized approach to gathering threat intelligence were more likely to report better risk management and emergency or crisis management outcomes. The results are less clear about a relationship between centralization and the areas of business continuity and overall organizational resilience.

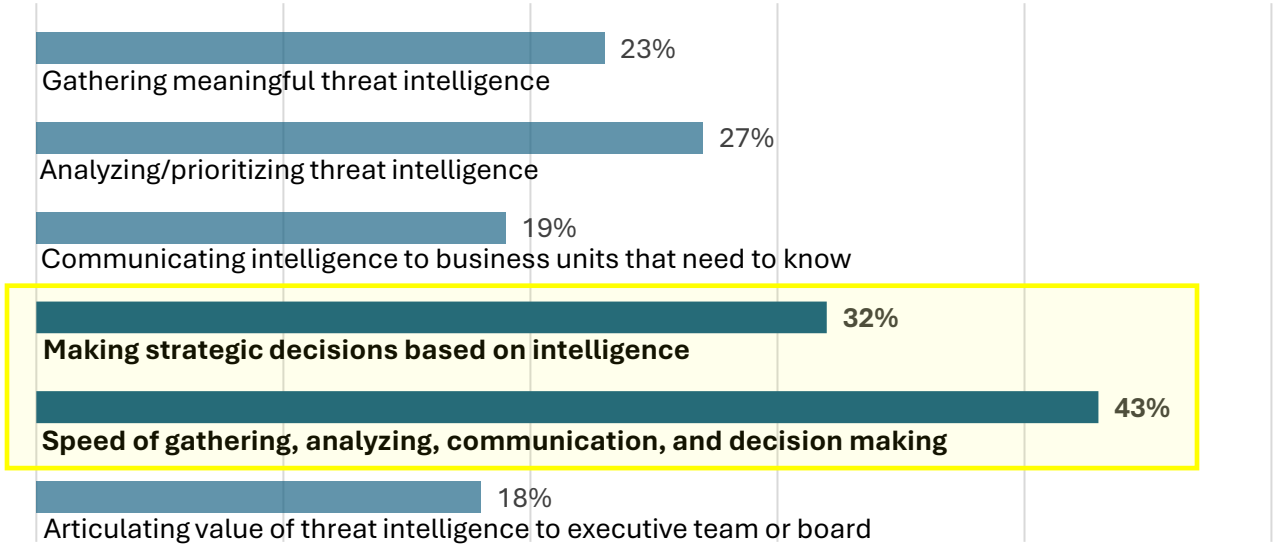
However, when examining the role security plays in threat intelligence, there is a stark contrast across all the areas: When security leads or plays a major role in threat intelligence gathering instead of a minor role or no role, outcomes in risk management, emergency or crisis management, business continuity, and overall organizational resilience are significantly better.

Mostly or Extremely Effective at Business Areas

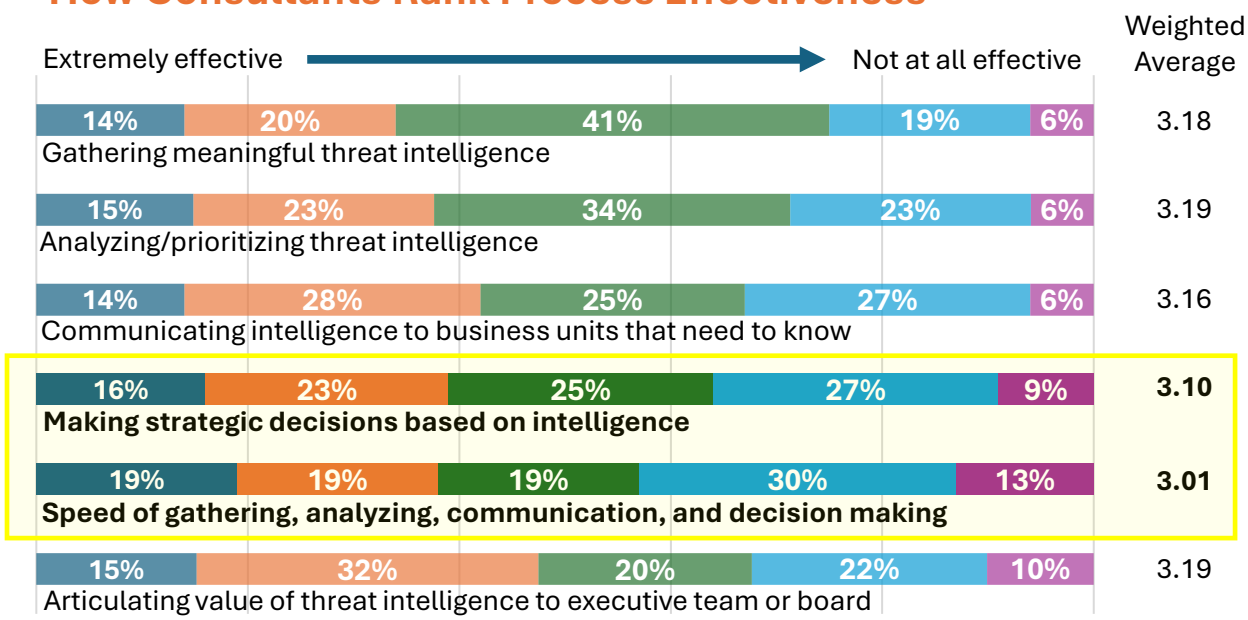




Consultants' Take: Areas Most Likely to Break Down and Lead to Significant Business Disruption



How Consultants Rank Process Effectiveness



From Security Consultants

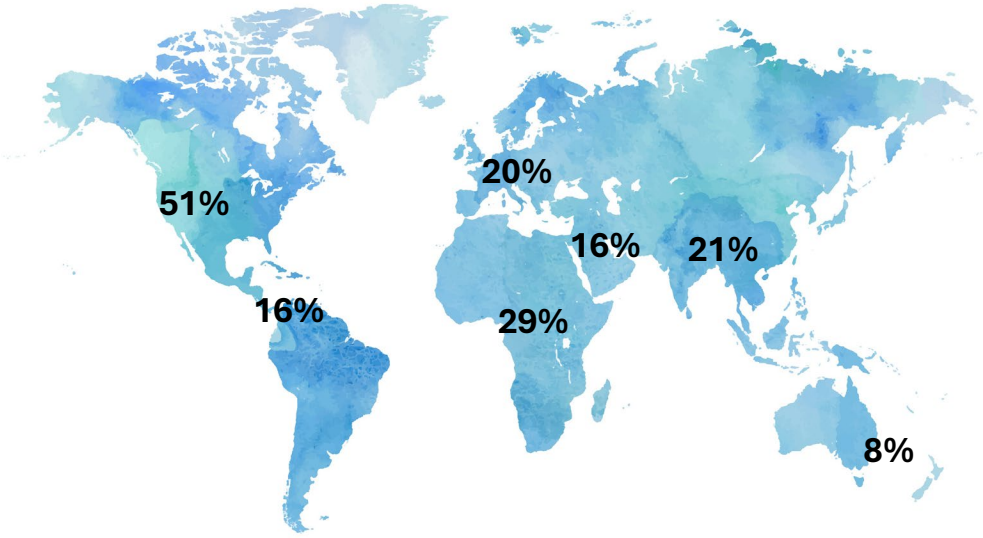
The survey gave security consultants the option to answer an alternate set of questions, and more than 100 did so.

One of the interesting findings from the consultants' survey was that the two parts of the intelligence process they rated as the most likely to break down and cause a disruption were also the two areas they rated as the weakest in the organizations they worked with (see highlights at left).

The consultants were also asked to provide their best advice on how organizations can improve threat identification and management. The following are some selected comments.

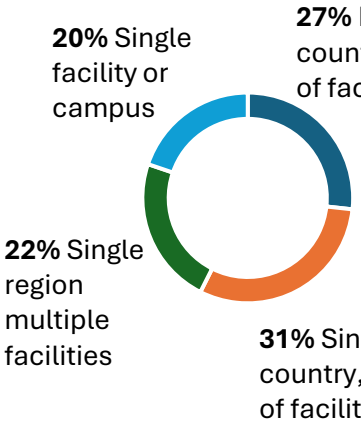
- My best advice to my clients is to include threat and risk assessment in every management meeting.
- Speed of predictive intelligence is critical to decision making.
- Have the proper qualified people doing the analysis and leave that team to provide an unbiased opinion of the threats rather than letting executives force their own opinions and slowing the process.
- Adopt a risk-based, integrated, and continuous approach to security, prioritizing threat intelligence and interdepartmental collaboration.
- Establish, budget for, train, and set benchmarks/expectations for a Threat Intelligence Unit within the organization.

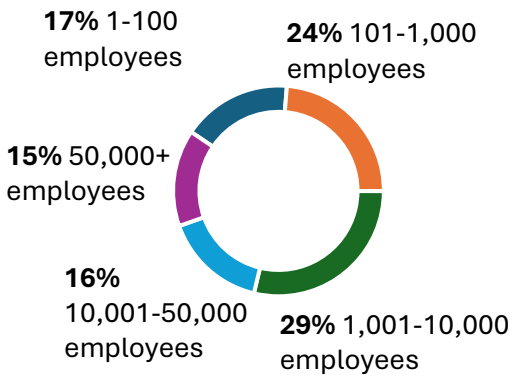
Survey Demographics: Geographic Scope



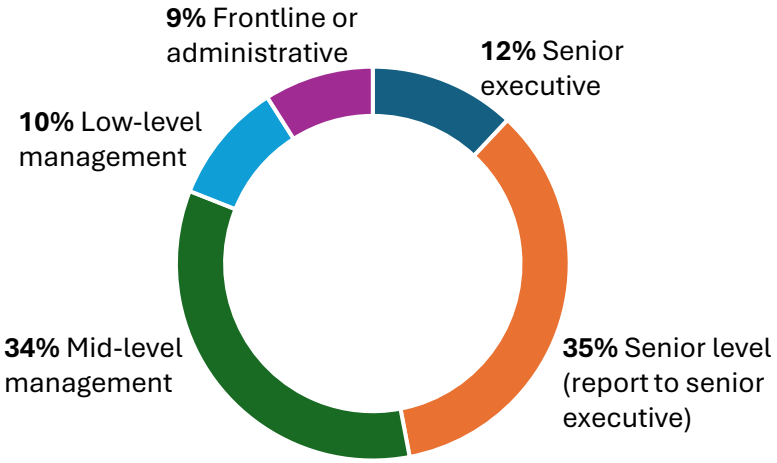
Participants were instructed to select all regions for which they had responsibility.

Organization Size and Scope





Position



Sector

Banking, Finance, and Insurance	8%
Manufacturing	7%
Oil, Gas, and Chemical	6%
IT and Telecommunication	6%
Education	5%
Healthcare	5%
Law Enforcement	5%
18 others less than 5% each	58%

Methodology

In the second quarter of 2025, ASIS International convened a small group of ASIS members and a representative from project sponsor Esri. This group put together a survey which was fielded in the month of June. The survey was promoted to ASIS members and customers via email, social channels, and ASIS newsletters. A total of 813 people answered at least some questions. All responses were recorded and used in this analysis regardless of whether the participant completed the survey. Security consultants and service providers were given the option to take an alternate set of questions. In total 531 people answered the last question available to them in the survey, which includes 104 consultant surveys and 427 standard surveys. Note: Some figures that should add to 100 percent do not because of rounding.

The margin of error for most questions in the standard survey is plus or minus 5 percent at the 95 percent confidence level. The margin of error for the consultant survey is plus or minus 10 percent, so the consultant results should be taken as a guide rather than as statistically significant research.

One source of bias could be that the survey was promoted as a threat intelligence and organizational resilience survey. People who self-select to take such a survey could reasonably be considered more knowledgeable about the topics than other security professionals and organization leaders. In addition, while the survey did not ask them to identify themselves, it is likely that a significant majority of the survey participants are ASIS members. This could also introduce bias because, similar to those who would self-select to take a survey based on its topic, ASIS is an organization dedicated to promoting best and promising practices in corporate security, and its members may have a more advanced knowledge of security concepts than nonmember security professionals.

ASIS would like to thank the following individuals for their assistance in developing the Threat Intelligence and Organizational Resilience Survey:

Eric Boger
Decode Risk

Michael Brzozowski, PSP, CPP
Google

Alex Martonik, MS, MBA
Esri

Brian Ishikawa, CPP
Bank of Hawaii

Tim McCreight, CPP
TaleCraft Security

Mike Moorman, CPP, PCI, CSMP
Yazaki North America

Jim Wooten
Geomark Consulting

The project lead was Scott Briscoe,
Content Development Director, ASIS International.