



Enterprise Strategy Group | Getting to the bigger truth.™

RESEARCH HIGHLIGHTS

An Ounce of Prevention: Investing in Incident Readiness

Jon Oltsik, Senior Principal Analyst and Fellow

AUGUST 2021

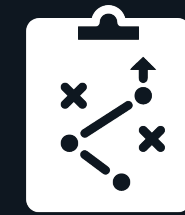
EXECUTIVE SUMMARY

[CLICK TO GO](#)



3

Research Objectives



4

Incident response plans should be formalized and supported.



7

Organizations see incident response retainers as a way to mitigate cyber risk.



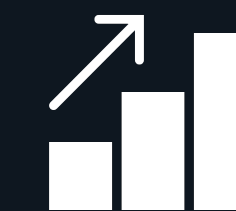
9

The cybersecurity skills shortage impacts incident readiness and response posture.



11

The people on the incident readiness frontlines must be skilled at communicating technical details concisely.



13

An ounce of prevention is worth a pound of cure when it comes to the benefits of investing in incident readiness.

Research Objectives

According to industry sources, there were more than 1,000 publicly disclosed data breaches in 2020, and the year ended with the devastating SolarWinds hack impacting 18,000 organizations worldwide. What can organizations do to protect themselves? Beyond basic technology preparedness actions such as penetration and vulnerability testing, many service providers have launched breach readiness programs to assist in aligning the organization, creating and practicing response playbooks and advanced simulation exercises.

In order to get more insight into the incident readiness market, ESG surveyed 334 IT and cybersecurity professionals at organizations in North America (US and Canada) responsible for the policies, processes, or technical safeguards used for incident readiness and response at their organization.

THIS STUDY SOUGHT TO:



Examine the impact of preparation for a breach on confidence and maturity of response.



Identify the best practices in the breach readiness market.

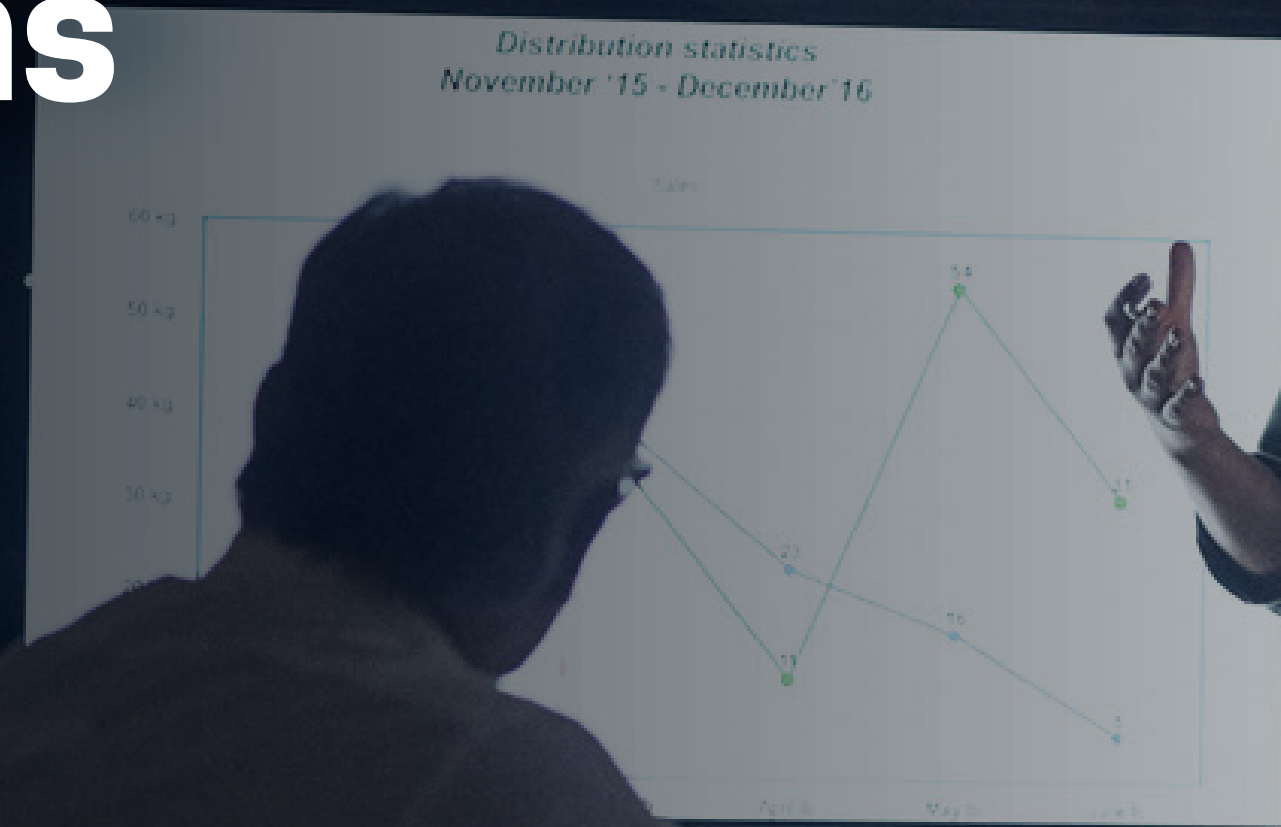


Discover drivers and efficacy of incident readiness services purchased.



Uncover preferences for different services according to various market segments.

**Incident response plans
should be formalized
and supported.**

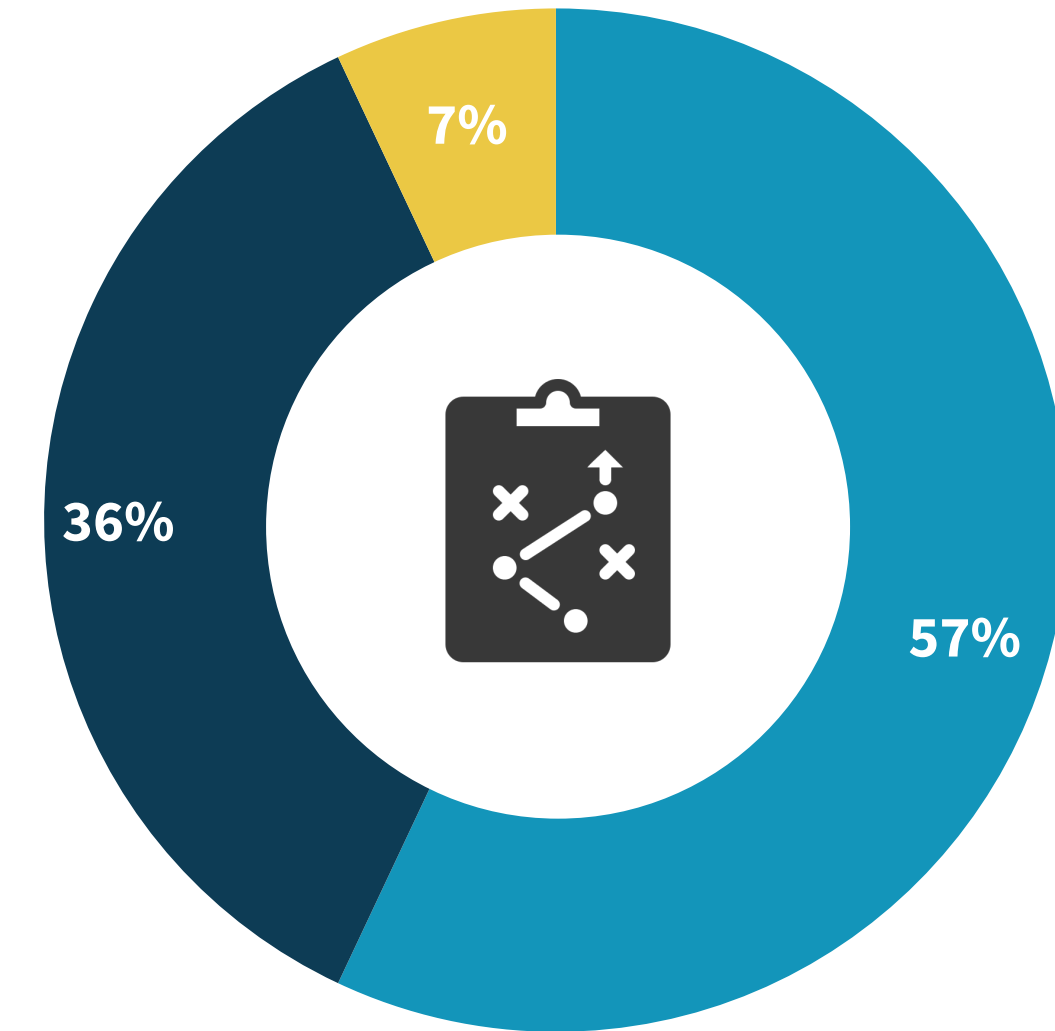


Slightly more than half have a documented response playbook, mostly integrated with standard operating procedures

An incident response playbook should be documented, tested, and fully integrated with standard operating procedures (SOPs). Given this model, the data paints a distressing picture as just more than half (57%) of organizations have a fully fleshed out and documented incident response playbook, while 55% claim that the incident response playbook is fully integrated with an SOP. That leaves lots of organizations with informal plans and procedures. This could lead to long cyber-attacker dwell times, lagging incident response, and haphazard organizational collaboration during a cyber-attack.

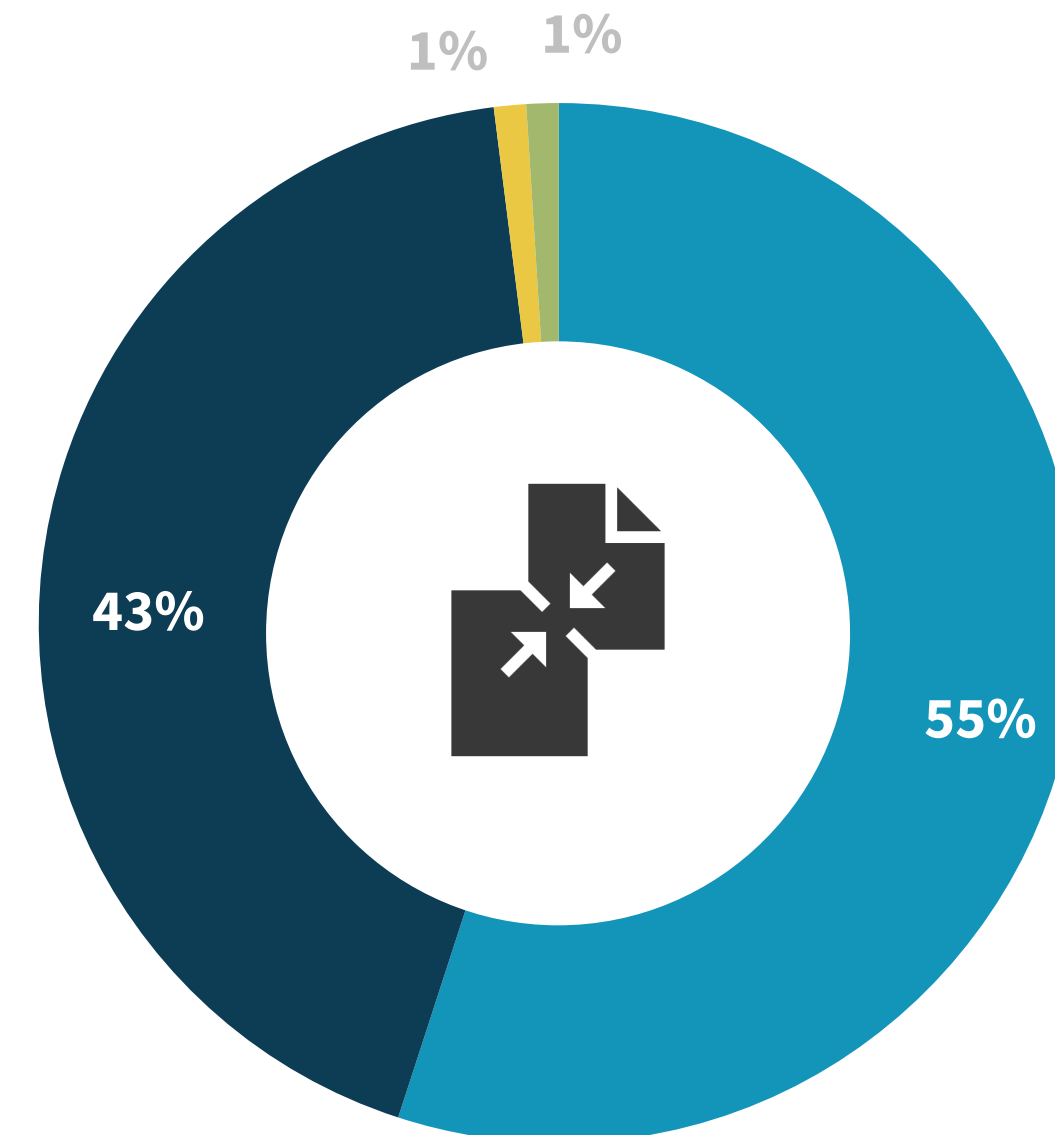
Incident response playbook status.

- Yes, we have a fully fleshed out and documented incident response playbook
- Yes, we have a documented incident response playbook, but it needs work
- No, we do not have a documented incident response playbook



Incident response playbook integration with SOP.

- Fully integrated with overall standard operating procedure (SOP)
- Somewhat integrated with overall standard operating procedure (SOP)
- Not at all integrated with overall standard operating procedure (SOP)
- Don't know




Organizations should fully integrate incident response playbooks and runbooks with SOPs


There is a strong correlation between incident response playbooks, as well as technical runbooks, and higher levels of confidence in the ability to respond to an incident. Not surprisingly, those that have fully documented incident response playbooks and technical response runbooks that are fully fleshed out and integrated with their organizations' standard operating procedures were significantly likelier to rate their ability to quickly detect and respond to cyber incidents as excellent. Specifically:

- Organizations that have a fully fleshed out and documented incident response playbook are **more than 3x likelier** than those that do not to rate their ability to quickly detect and respond to cyber incidents as excellent.
- Organizations that have fully integrated their incident response playbook with overall standard operating procedure are **more than 6x likelier** than those that have not to rate their ability to quickly detect and respond to cyber incidents as excellent.
- Organizations that have a fully fleshed out and documented technical runbook are **nearly 4x likelier** than those that do not to rate their ability to quickly detect and respond to cyber incidents as excellent.

| Percentage of organizations rating their ability to quickly detect and respond to cyber incidents as excellent.

 **49%**


We have a fully fleshed out and documented incident response playbook.

 **55%**

We have fully integrated with overall standard operating procedure (SOP).

 **53%**

We have a fully fleshed out and documented technical runbook.

A photograph of three people in a dimly lit office environment. One person is pointing at a computer monitor, while two others look on. The scene is illuminated by the glow of the screen and a desk lamp. The overall mood is focused and collaborative.

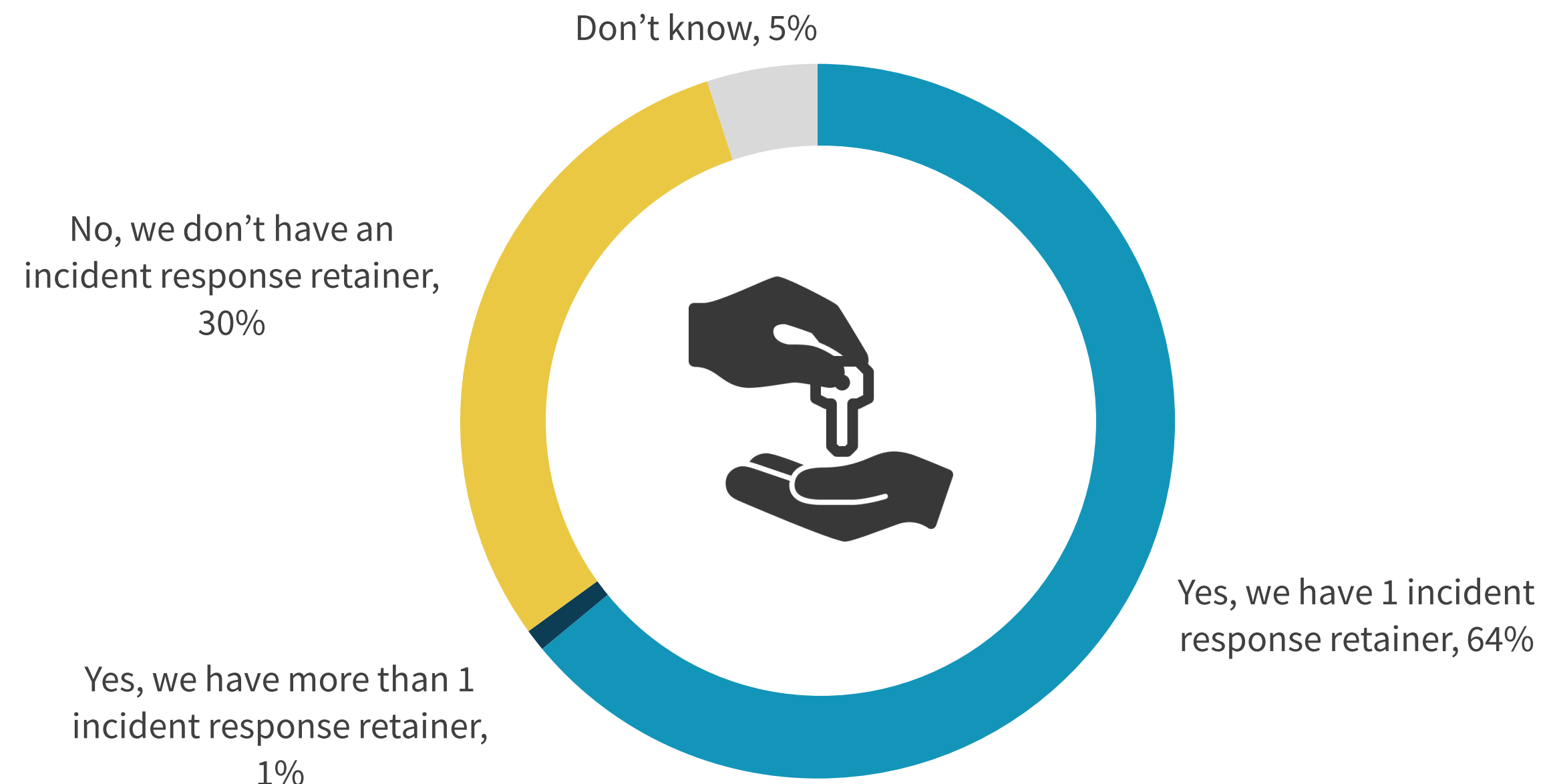
Organizations see incident response retainers as a way to mitigate cyber risk.

Most have an incident response retainer, with a breach notification communication plan cited as a key incident response playbook output

Most companies have at least one retainer to assist with breach response, but 30% have none. This means that these firms are relying on their own internal skills and processes. This may be acceptable for well-resourced enterprise organizations, but unacceptable for resource-constrained firms with immature security processes. Given the global cybersecurity skills shortage and recently announced vulnerabilities and sophisticated cyber-attacks, going it alone may be a fool's errand.

“Most companies have at least one retainer to assist with breach response, **but 30% have none.**”

| Existence of incident response retainers.



The cybersecurity skills shortage impacts incident readiness and response posture.



Cybersecurity skills shortage spills over into incident readiness

ESG’s 2021 technology spending intentions survey confirms that nearly half of respondents feel that there is a problematic skills shortage in cybersecurity.¹ This global skills shortage impacts many cybersecurity tasks, including incident readiness, making organizations more susceptible to data breach events. Not surprisingly, more than four in ten cite personnel issues among their organization’s weakest areas of incident readiness in terms of both supply and skill set.

Additionally, organizations feel their weakest links are information sharing and intelligence, conflicting priorities for the security team, and lack of resources (both human and budgetary).

“**Nearly half** of respondents feel that there is a problematic skills shortage in cybersecurity.”

| Weakest areas of cyber incident readiness and response.



The people on the incident readiness frontlines must be skilled at communicating technical details concisely.

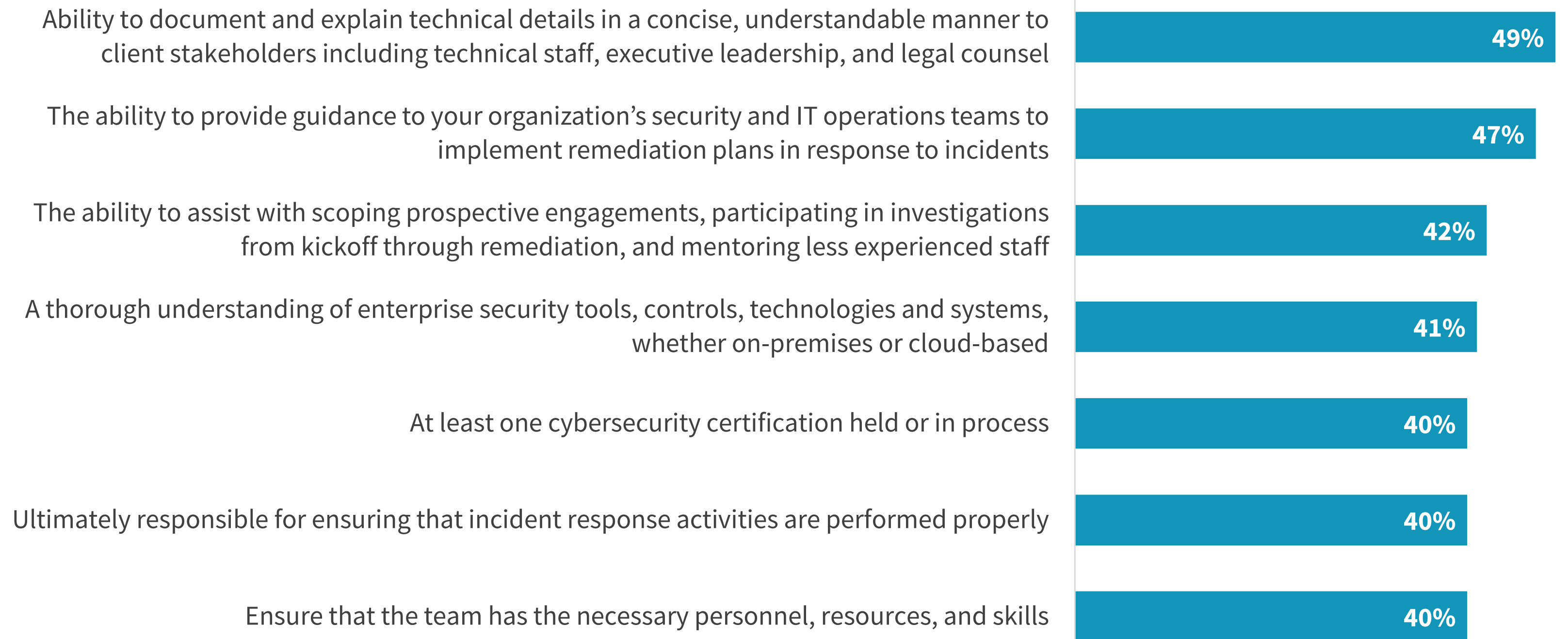


Incident response leader: communication & management skills outweigh tech skills

Interdepartmental communication skills between both the business and engineering/IT teams and the IT operations and security teams is a foremost knowledge, skills, and abilities (KSA) metric for incident response leaders. For example, nearly half (49%) of organizations believe that security/IT teams must be able to document and explain technical details in a concise and understandable manner, while 47% believe these teams must have the ability to guide technical teams through remediation processes. These are acquired skills that tend to be learned and fine-tuned over time. CISOs and CIOs must assess whether their organization has mature skill sets in these areas or not.

Clearly, organizations recognize a gap between current and ideal incident readiness. To improve existing processes and procedures, three in four organizations will increase spending on incident readiness exercises.

Knowledge, skills, and abilities expected of incident response leaders.



Spending change for incident readiness exercises.



Will your organization increase or decrease its spending with service providers on incident readiness exercises in the next 12 to 18 months?

32%

Spending will increase significantly

43%

Spending will increase somewhat

An ounce of prevention is worth a pound of cure when it comes to the benefits of investing in incident readiness.





Taking proactive measures is vital to any aspect of a strong cybersecurity strategy, especially when it comes to incident readiness and response capabilities. Having the combination of technologies, processes, and personnel in place prior to the occurrence of a security incident helps to ensure a greater likelihood of successful mitigation and recovery.

Through its acquisition of the Crypsis Group, Palo Alto Networks Unit 42 brings together cybersecurity researchers and incident responders to protect mission-critical digital assets. In addition to leading threat intelligence, Unit 42 now provides a range of incident response and cyber risk management services, where consultants serve as trusted partners to respond quickly, contain threats completely, and help customers restore business operations.

CYBER RISK MANAGEMENT

- Compromise Assessment
- Breach Readiness Review
- Board Advisory Services

THREAT INTELLIGENCE

- Threat Briefings
- Actionable Threat Objects & Mitigations (ATOMs)
- Cyber Threat Intel Tools

DIGITAL FORENSICS & INCIDENT RESPONSE (DFIR)

- Ransomware Investigation
- Business Email Compromise
- Digital Investigations

[LEARN MORE](#)

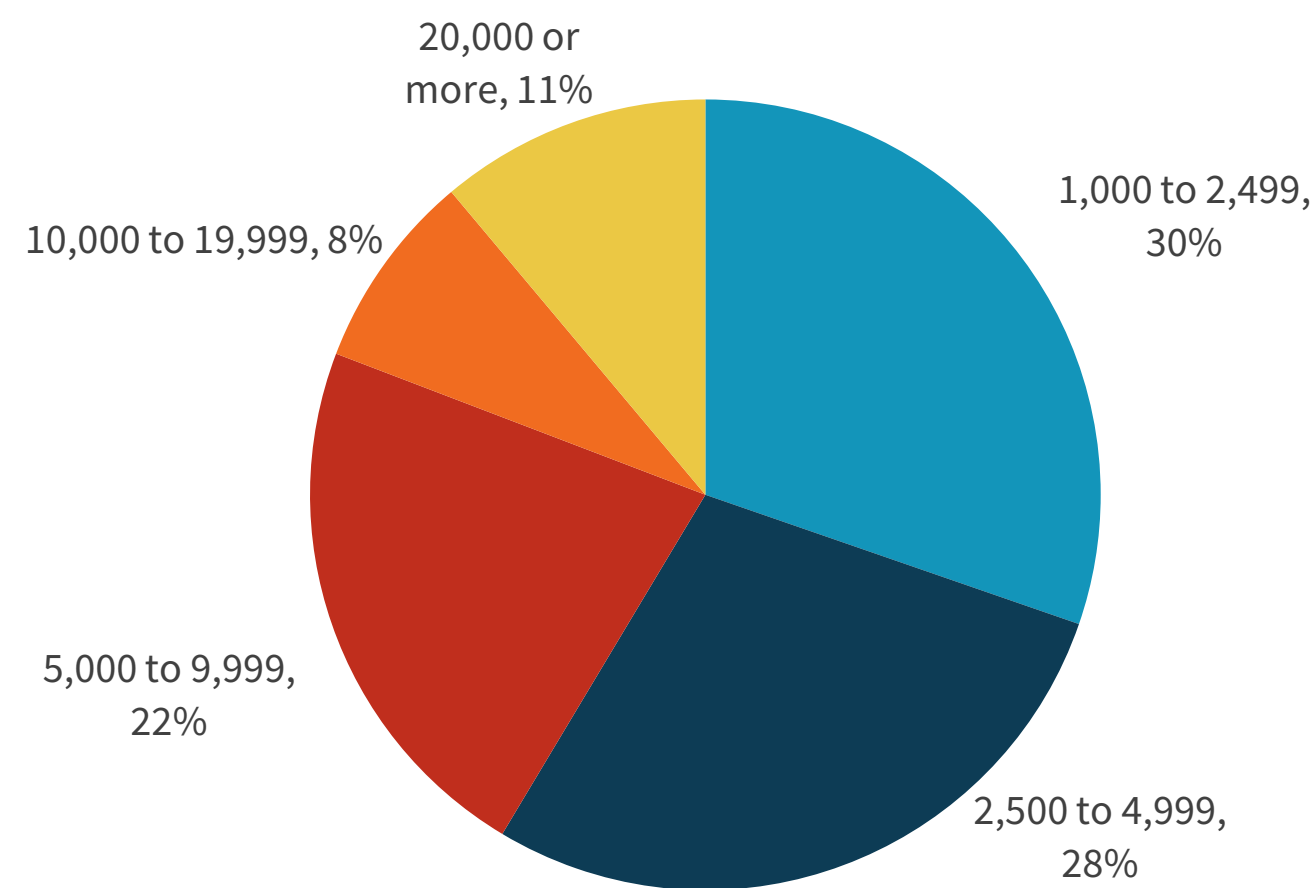


Research Methodology

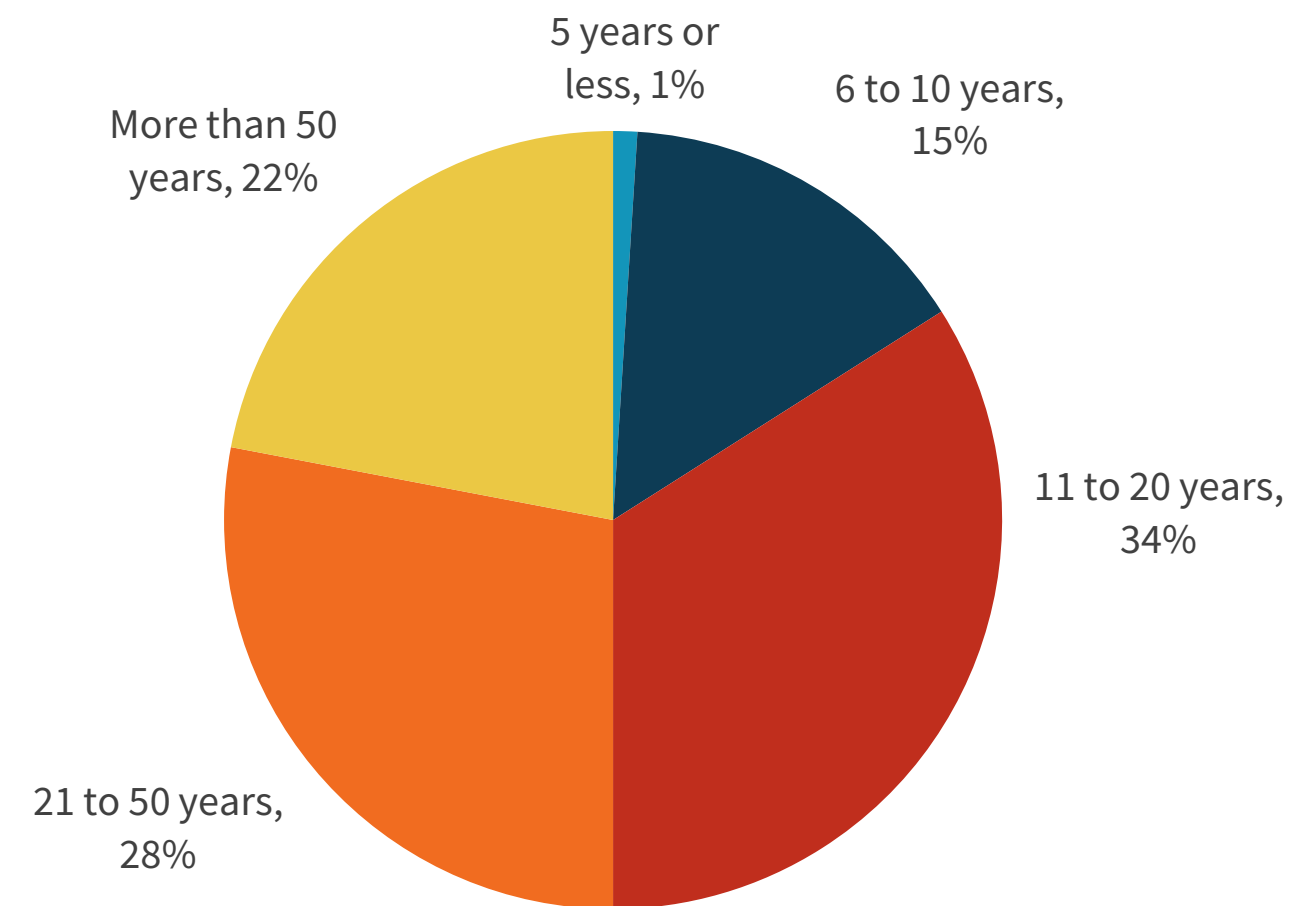
To gather data for this report, ESG conducted a comprehensive online survey of IT and cybersecurity professionals from private- and public-sector organizations in North America (United States and Canada) between June 25, 2019 and July 7, 2019. To qualify for this survey, respondents were required to be IT or cybersecurity professionals personally responsible for the policies, processes, or technical safeguards used for incident readiness and response at their organization. All respondents were provided an incentive to complete the survey in the form of cash awards and/or cash equivalents.

After filtering out unqualified respondents, removing duplicate responses, and screening the remaining completed responses (on a number of criteria) for data integrity, we were left with a final total sample of 334 IT and cybersecurity professionals.

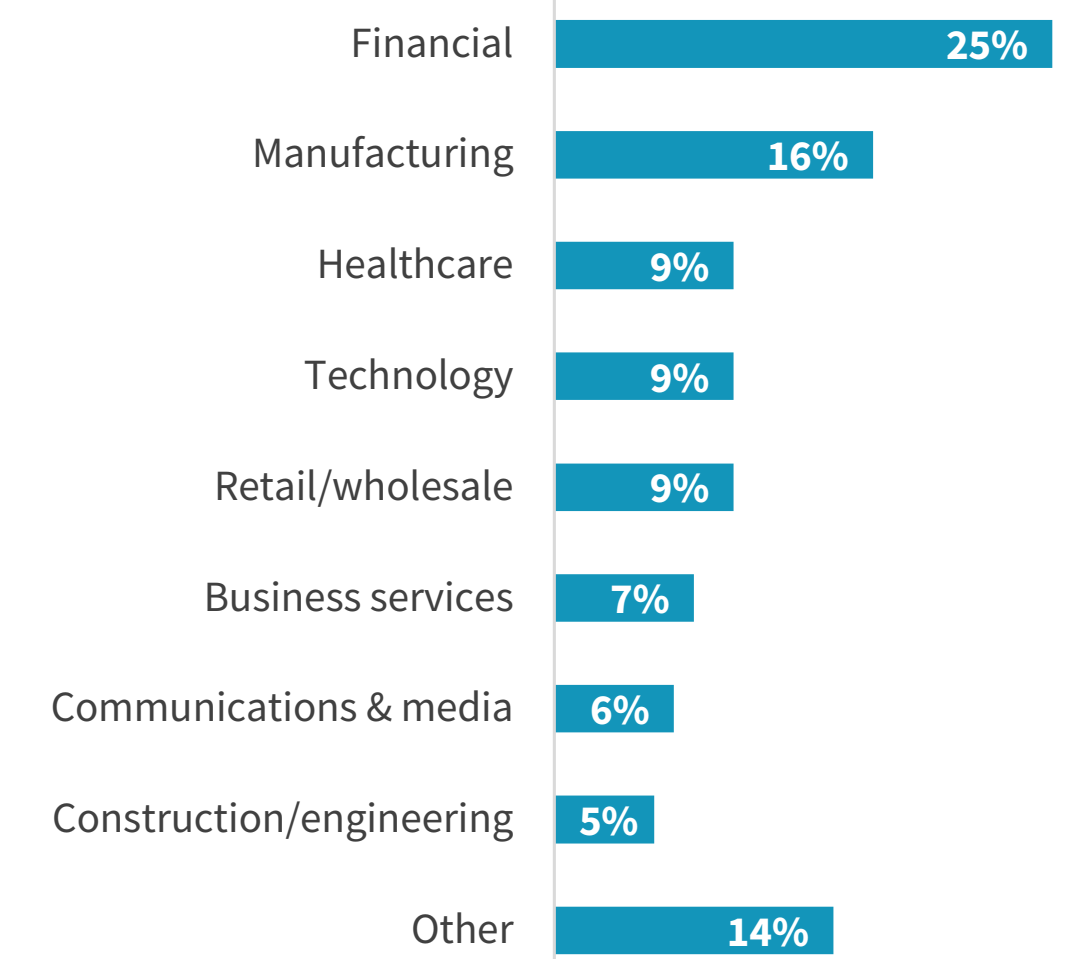
RESPONDENTS BY NUMBER OF EMPLOYEES



RESPONDENTS BY AGE OF COMPANY



RESPONDENTS BY INDUSTRY



All product names, logos, brands, and trademarks are the property of their respective owners. Information contained in this publication has been obtained by sources TechTarget, Inc. considers to be reliable but is not warranted by TechTarget, Inc. This publication may contain opinions of TechTarget, Inc., which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget, Inc.'s assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget, Inc. makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

This publication is copyrighted by TechTarget, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of TechTarget, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact Client Relations at cr@esg-global.com.



Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.

© 2021 TechTarget, Inc. All Rights Reserved.