Enterprise Strategy Group™ by TechTarget

# Incident Response Strategies in the Spotlight

**Dave Gruber,** Principal Analyst
ENTERPRISE STRATEGY GROUP

# Research Objectives

Ransomware, business email compromise, and other attacks are increasingly evading cybersecurity defenses, causing IT and cybersecurity teams to further invest in incident response (IR) readiness. As such, IR can no longer be viewed as an event-driven action but must be operationalized and become a core strategy within security operations. As security and line-of-business teams react to this new reality, new IR strategies are needed for most.

Few have the internal resources and capacity to handle this key function on their own, requiring many to leverage a service-based approach. While managed security service providers and managed detection and response service providers have become commonplace, a deeper partnership is needed to enable real-time IR services capable of mitigating damage from successful attacks. Cybersecurity leaders need to better understand the differentiation of IR services as a standalone offering, versus those included in a broader set of service offerings, to make more informed decisions.

To gain further insight into these trends, TechTarget's Enterprise Strategy Group surveyed 339 IT and cybersecurity professionals at organizations in North America (U.S. and Canada) involved with IR technologies and processes.

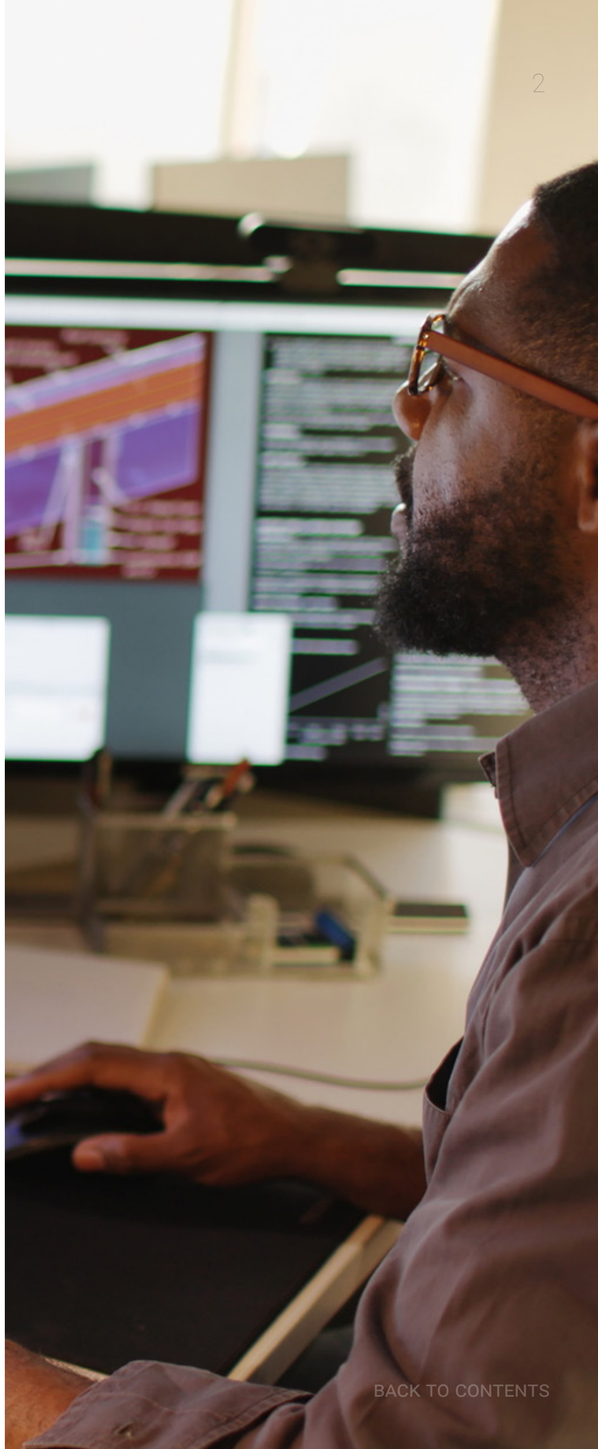
**This study sought to:**

**Assess** the state of IR strategies and readiness activities.

**Validate** IR best practices through the creation of cohorts, identifying the types of organizations and notable dynamics that yield the most (and least) effective IR activities.

**Determine** the status of IR strategies, how organizations measure readiness, and who they are partnering with to develop and execute IR activities.

**Highlight** notable gaps or challenges organizations are struggling with as they strengthen IR readiness initiatives and opportunities for security vendors to help overcome them.





BACK TO CONTENTS

# KEY FINDINGS

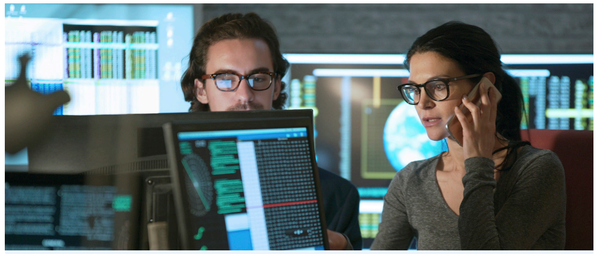
CLICK TO FOLLOW

**Despite Continued Security Program Investments, Attack Success Persists, Driving the Need for IR Strategies**

PAGE 4

**IR Services and Strategies Are Evolving and Expanding in Scope**

PAGE 8



**IR Preparedness Requires a Highly Collaborative Effort**

PAGE 12

**IR Service Providers Are Delivering Value Beyond Containment and Recovery**

PAGE 16

**IR Services Engagements Require Upfront Planning**

PAGE 20

**Urgency Exists in IR Preparedness, Driving Increased Investment**

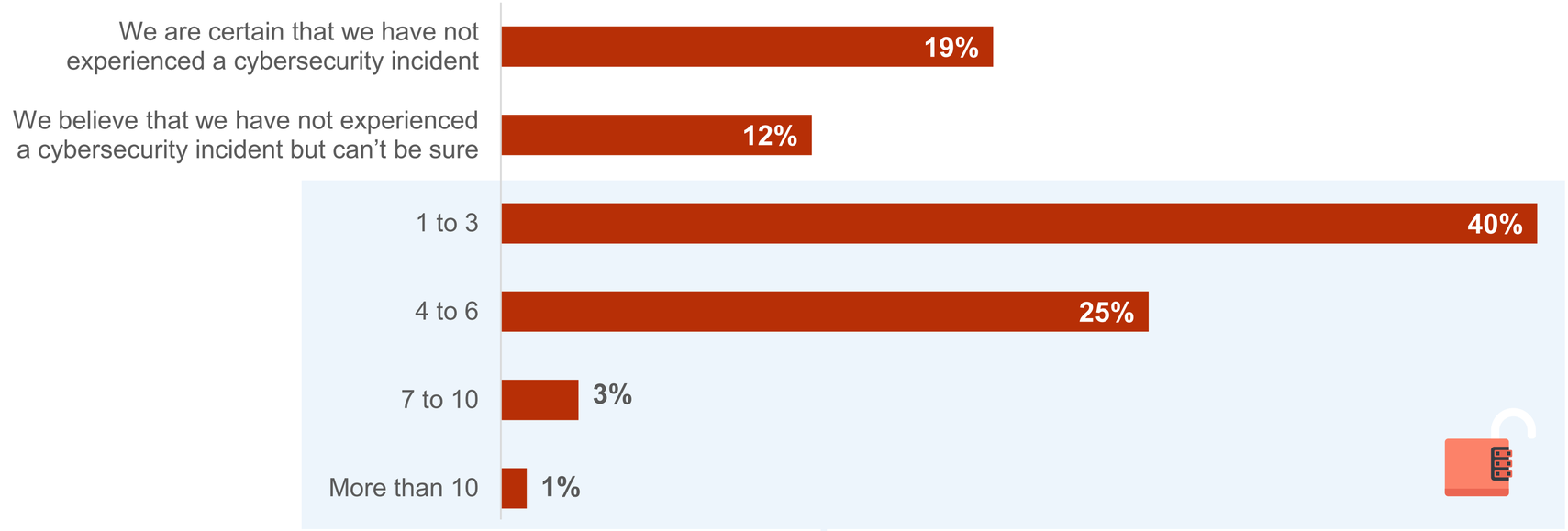
PAGE 24

# Despite Continued Security Program Investments, Attack Success Persists, Driving the Need for IR Strategies

# More than Two-thirds Report Damaging Attacks Caused by Cyber Incidents

Despite ongoing focus on and investment in strengthening cybersecurity programs, attackers continue to successfully penetrate defenses, with damaging outcomes. Specifically, more than two-thirds of organizations have experienced at least one cyber incident within the last two years, and the vast majority of these organizations indicate that at least one of these attacks was damaging. Operational disruption, financial impact, data loss, sensitive data exposure, and reputational damage are but a few of the types of damages involved, making incident response readiness a critical strategy to minimize these impacts.

Number of cyber incidents experienced over the past two years.




Number of **damaging** attacks experienced by cyber incident victims over the past two years.




BACK TO CONTENTS

# Missteps Abound When Responding to Cyber Attacks

Digital forensics teams' IR skills and processes are lacking, resulting in far more time spent on forensic investigation than anticipated. And IR readiness extends beyond internal skills and processes, requiring collaboration with law enforcement agencies, regulatory bodies, and legal teams. On a more positive note, missteps often lead to the identification and closure of gaps in many areas, shining a light on the people, processes, technology, and communication plans required to effectively respond to critical situations. So, while the pain is often significant during the first attacks, IR programs improve over time with experience and through the guidance of third-party experts who are often engaged to help.

Missteps experienced when responding to cyber attacks.

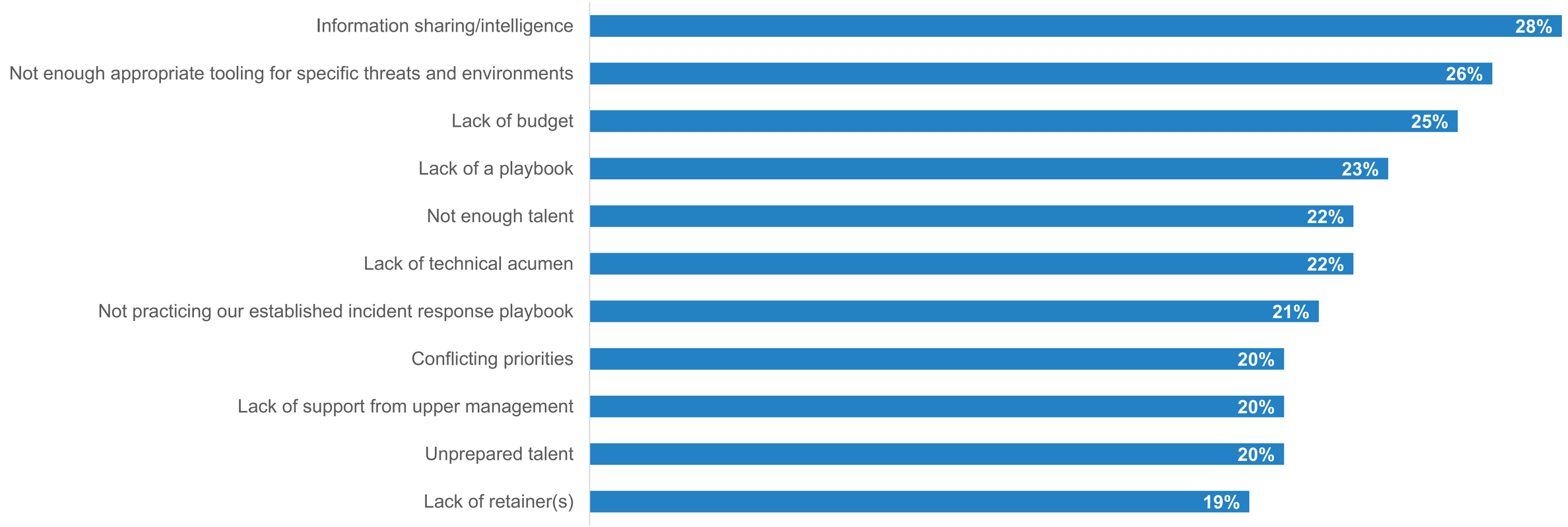



BACK TO CONTENTS

# Weaknesses Are Common in IR Preparedness, Including Skills Gaps, Tooling Gaps, and Process Gaps

Despite the breadth of challenges, the most common cyber IR-related  weakness reported is the ability to share information and intelligence as an incident unfolds. IR is a crisis for many, where response time directly impacts the extent of the damage done, so well defined, well rehearsed communication and collaboration plans are critical. Every individual involved needs to understand their role, the role of others, and the playbook for what needs to be done. Preparedness is key, including having rehearsed all aspects of incident response.

Weakest areas of cyber IR.






BACK TO CONTENTS

# IR Services and Strategies Are Evolving and Expanding in Scope

# IR Services Are Available Through Many Avenues

Once the role of only a few highly trained specialized IR service providers, present-day IR services are offered by a variety of security service providers, including core security technology solution providers offering add-on IR services; dedicated, specialized IR service providers; broad systems integrators; and the rapidly growing use of managed detection and response service providers, who also offer IR services as an add-on retainer. Most service providers offer both an “on-demand, as needed” event-based service and a retainer-based offering, supporting those most prepared in addition to those caught in crisis.

Type of security service provider supporting IR needs.

**61%**

A security technology solution provider that also operates an IR service

**53%**

A systems integrator that offers an IR services retainer or event-based service

**47%**

An MDR provider that offers IR services as an add-on retainer

**37%**

Dedicated, specialized IR service provider

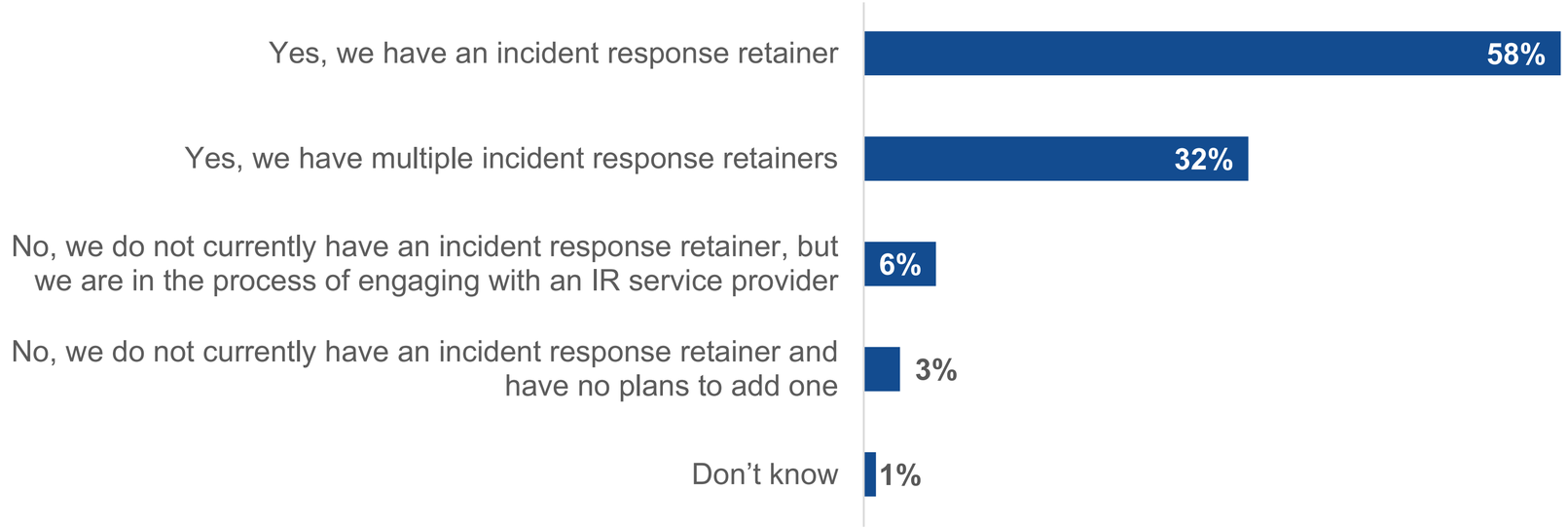


BACK TO CONTENTS

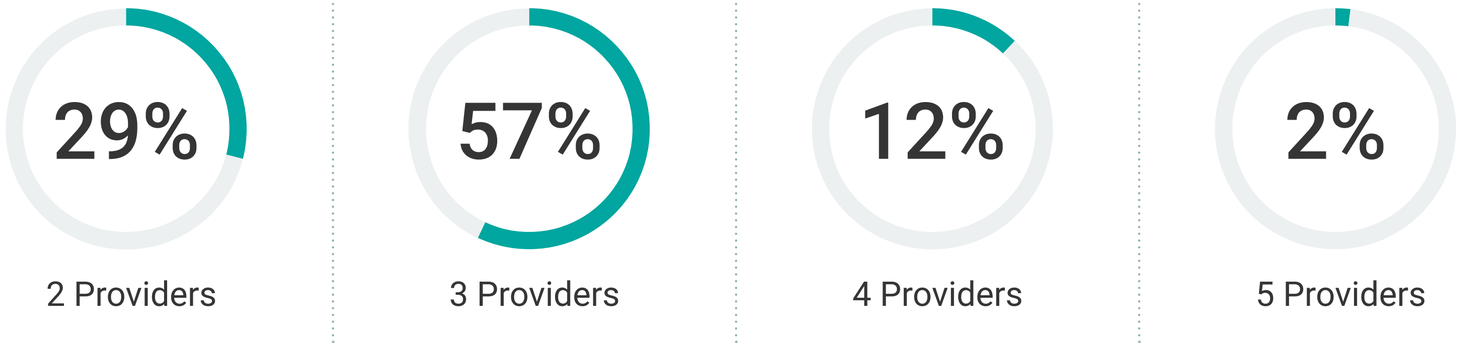
# Majority of Organizations Have an IR Retainer and One-third Engage With Multiple IR Providers

IR retainers are becoming more commonplace, enabling IT and security teams to work together with IR service providers in the preparation process. The vast majority of organizations have at least one IR retainer, with almost one-third (32%) utilizing multiple IR service providers to fill specific needs of the organization. When IR service providers are retained, they can work together with organizations to strengthen preparedness, including activities such as endpoint detection and response services, cybersecurity maturity assessment, IR plan and playbook development, data recovery and forensics analysis, security posture assessments, response readiness assessments, and more.

Do organizations currently have an active IR retainer?




Number of IR retainers organizations have.



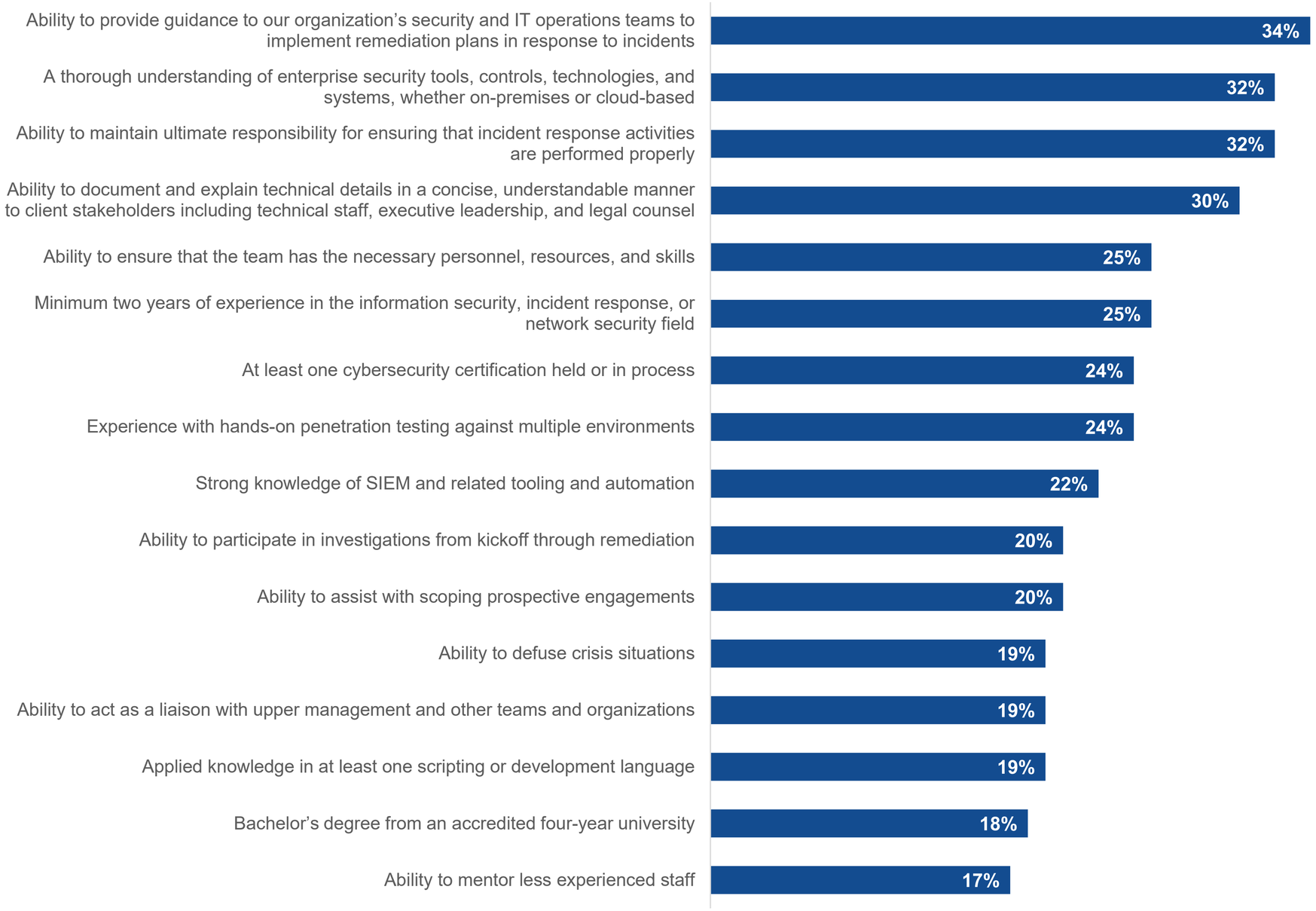



BACK TO CONTENTS

# Much Is Expected From Those Involved in Incident Response

What is expected of IR leaders? First and foremost is the ability to provide guidance to security and IT operations teams to implement remediation plans in response to incidents. As an IR “commander,” a thorough understanding of enterprise security tools, controls, technologies, and systems is required, both those on premises and those operating in the cloud. Communication skills are a must, as IR leaders must inform and guide all stakeholders, across technical, legal, and executive staff.

KSAs expected from IR leaders.






BACK TO CONTENTS

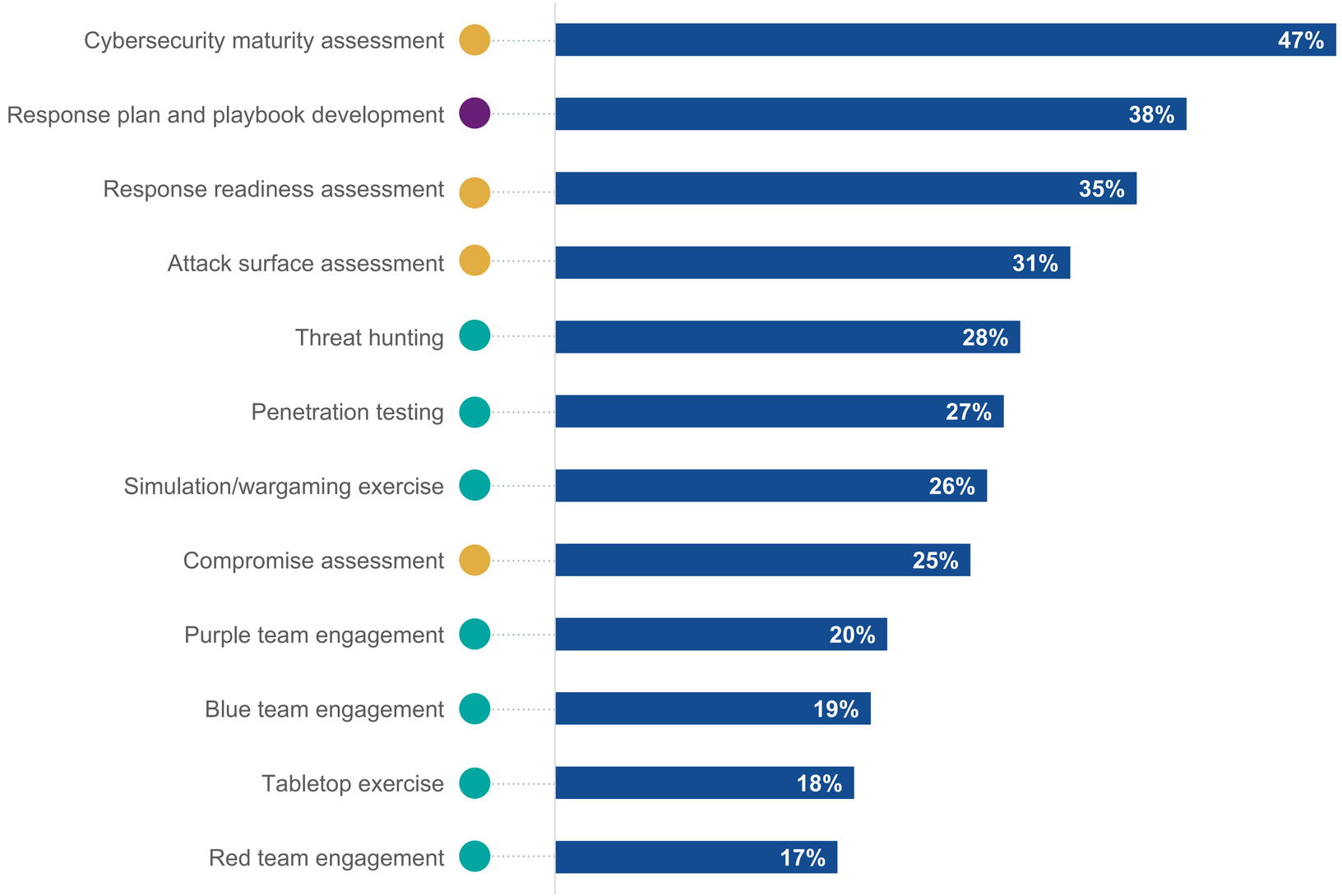
# IR Preparedness Requires a Highly Collaborative Effort

# IR Readiness Activities Undertaken Within Past 12-18 Months

IR readiness involves multiple assessments, planning, and proactive testing activities. While many types of assessments are in use, cybersecurity maturity assessments top the list, with almost half of respondents reporting that they have used them. Once created, IR response plans and playbooks are validated through testing activities. Proactive testing includes both event-based activities and operationalized functions, such as red/blue/purple-team exercises, tabletop exercises, attack simulation exercises, and ongoing threat hunting, attack surface assessment, and penetration testing.

- **Assessments**
- **Plans**
- **Proactive testing**

IR readiness activities organizations have engaged in over the last 12-18 months.






BACK TO CONTENTS

# IR Readiness Involves In-house and External Resources

Who performs IR readiness activities? A combination of internal staffing and third-party services are commonly used. This is true across almost all aspects of IR readiness, tipping more toward third-party providers for threat hunting, penetration testing, attack surface assessment, and purple team engagement activities. Despite the high commitment to in-house staffing, most need help with skills, processes, and technologies in one or more areas of their program.

IR readiness activities: in-house staff versus third-party service providers.




BACK TO CONTENTS

# IR Improvement Plans

How are organizations planning to strengthen their IR readiness? Topping the list is the use of more expert service providers that can help assess and improve readiness processes. More formally retaining an IR service provider is high on the list, with an emphasis on reviewing, updating, and documenting IR processes. And because threat intelligence arms organizations with what they need to defend against, consuming and analyzing more external threat intelligence is also a priority.

Actions organizations will likely take over the next 12-18 months to improve IR readiness.

**47%**
Work with professional services to help us assess and improve incident readiness processes

**42%**
Develop more formally documented threat detection and incident response processes

**39%**
Consume and analyze more external threat intelligence (open source and commercial)

**39%**
Put an incident response service on retainer

**35%**
Share information with like-minded organizations

**29%**
Adopt MDR services

**29%**
Hire/train more security analysts



BACK TO CONTENTS

# IR Service Providers Are Delivering Value Beyond Containment and Recovery

# IR Service Providers Helped in Multiple Ways During Recent Attacks

IR service providers are delivering value beyond threat containment, the identification of impacted assets, and the recovery of compromised systems and data. IR providers are further guiding and managing communications processes, both internally and externally, in addition to helping to negotiate with criminals to minimize financial impact. And coming out of the engagement, IR providers are leveraging their digital forensics' investigation and response process to identify weaknesses in security controls and make recommendations to improve them.

How IR service providers assisted during most recent attacks.

**40%**
Identified security control weaknesses and made recommendations to improve them

**35%**
Helped recover compromised systems and data to restore the operation

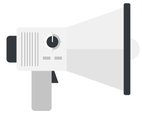
**35%**
Completed a forensics investigation that identified the assets affected

**34%**
Provided easy-to-follow, respectful, and compassionate service

**33%**
Collaborated with internal IT resources to establish a clean operating environment

**33%**
Engaged services in a timely manner, and identified and contained the attack

**27%**
Managed crisis communications internally



**24%**
Guided our external communications process

**21%**
Helped negotiate with criminals to minimize financial impact

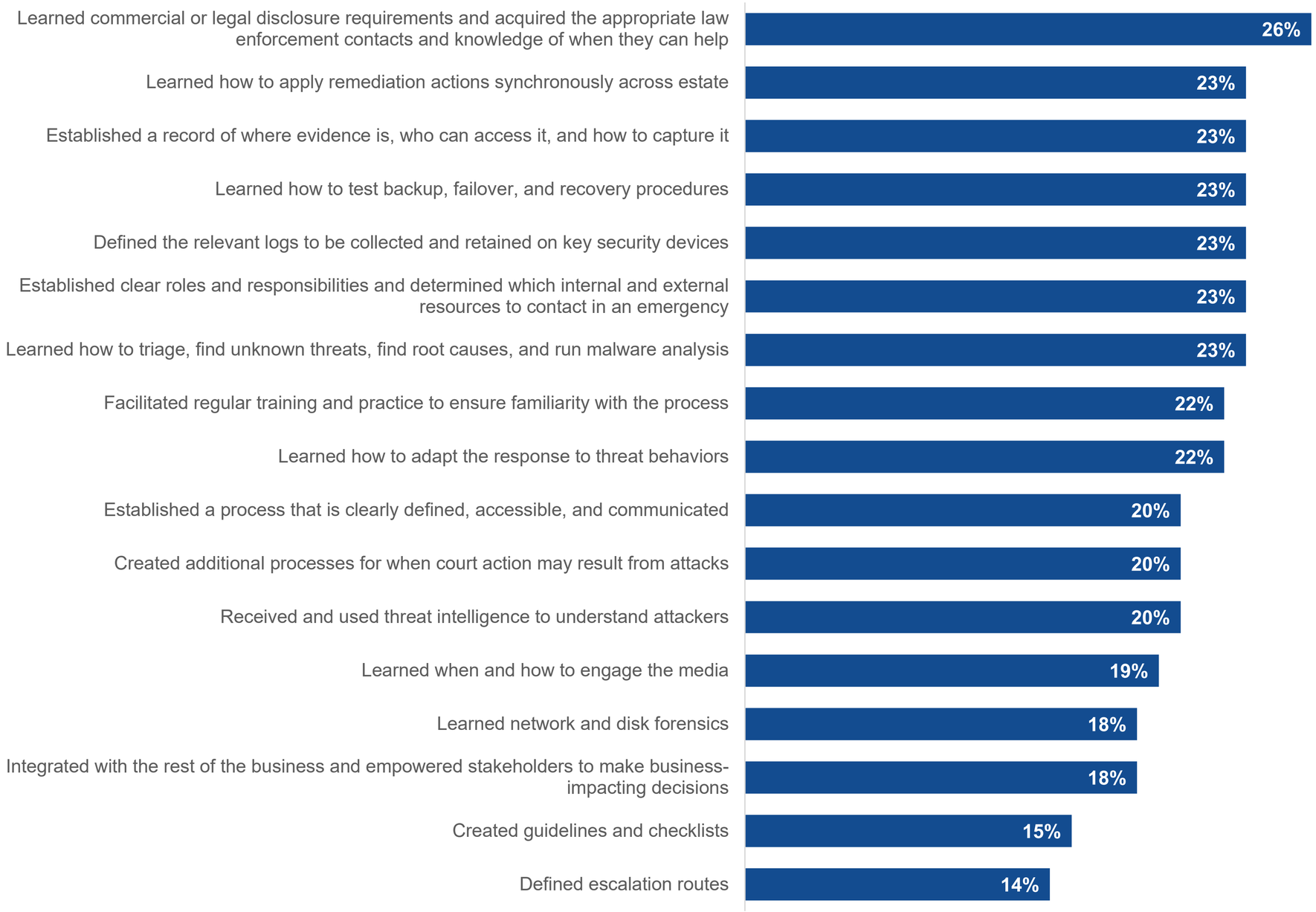


BACK TO CONTENTS

# Post-event Benefits Extend Beyond Containment and Recovery

IR service providers are leaving behind valuable, newfound knowledge for internal IT, security, and line-of-business teams, strengthening readiness. Learning commercial or legal disclosure requirements and acquiring law enforcement relationships and contacts lay the groundwork for moving faster for future events. IR service providers are further credited with teaching organizations where and how they need to test readiness activities, as well as backup and recovery systems and processes, how and where to find and capture evidence, and more.

Benefits realized as a result of engaging with an IR service provider.



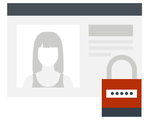



BACK TO CONTENTS

# Unexpected – But Positive – Results of IR Engagements

In addition to benefits realized, there were also a number of unexpected outcomes derived from IR service engagements. Internal security resources report advancing their own skills in IR operations and execution, which better prepares them for future incidents. A long list of identified gaps and recommendations to improve visibility, systems, processes, and skills were also seen as expected benefits. New insights into exposing supply chain security issues came to light, as did the importance in strengthening vulnerability management activities.

Unexpected outcomes achieved as a result of most recent IR engagements.

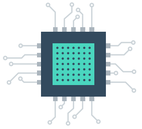


**30%**
Internal security resources advanced their skills in IR operations and execution

**27%**
Identified specific security program gaps

**27%**
Initiated an attack surface management program

**26%**
Identified and closed visibility gaps in specific parts of our attack surface



**26%**
Identified specific technology weaknesses in our current security tech stack

**25%**
Identified rogue/unknown infrastructure without security controls or visibility in place

**25%**
Formalized IR readiness activities

**25%**
Exposed supply chain security issues

**24%**
Recognized lack of IR preparedness

**24%**
Increased focus on our vulnerability management program

**22%**
We engaged with an MDR service provider

**20%**
Developed a formal IR readiness program



BACK TO CONTENTS

# IR Services Engagements Require Upfront Planning

# IR Provider Selection Criteria

What are organizations looking for in an IR service provider? Compatibility starts with experience, beginning with like-industry and security tools stack experience. Not surprising, depth of knowledge in the threat landscape and the number of successful IR engagements completed to date both play a key role in the selection process. As cyber insurance becomes a key risk-mitigation strategy, it makes sense that more than one-quarter (29%) of organizations reported receiving recommendations for IR service providers from their cyber insurance providers.

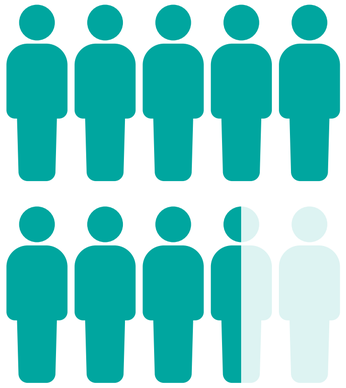
Criteria used in selection process for current IR providers.




BACK TO CONTENTS

# Cyber Insurance Is Prevalent and Influencing IR Engagements

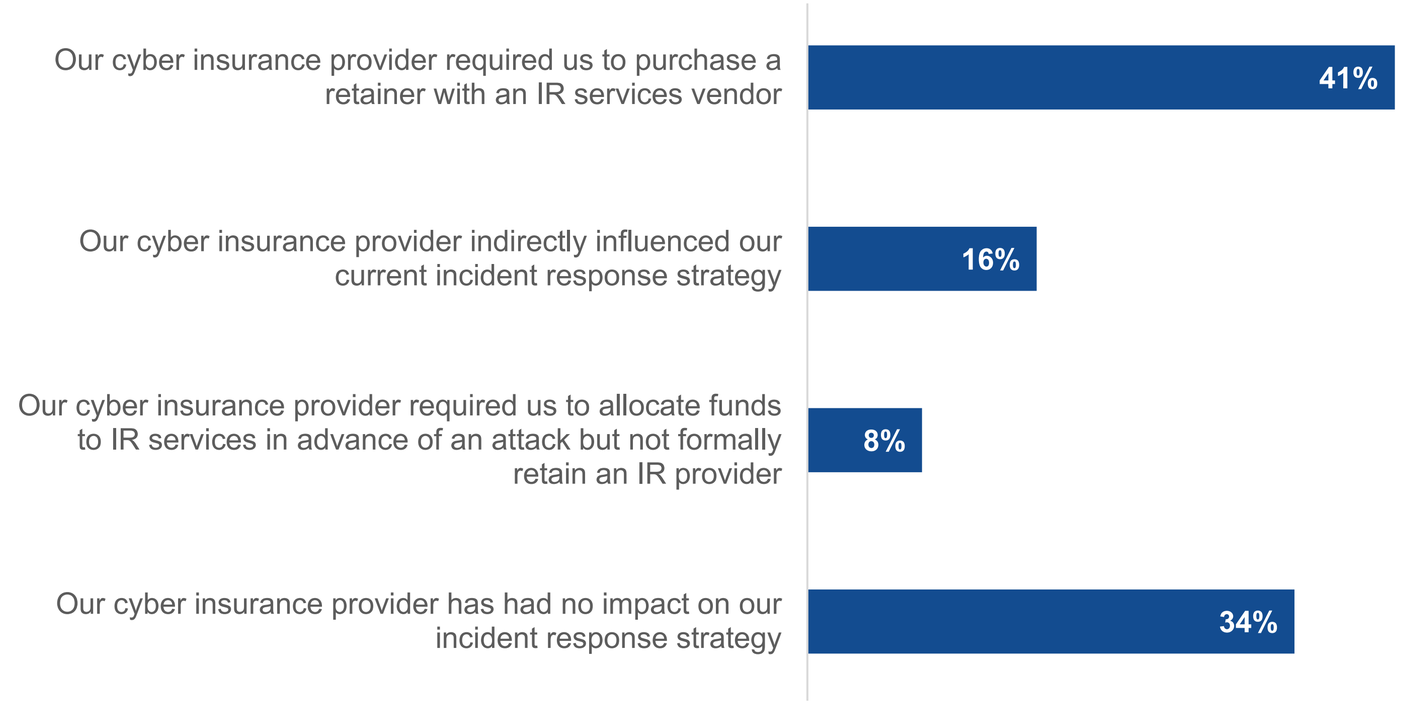
While more than a quarter of organizations reported receiving IR provider recommendations from their cyber insurance provider, many more indicated influence was being exerted. Indeed, among the 84% of organizations currently using cyber insurance as part of their risk mitigation strategy, more than half were motivated by cyber insurance requirements to retain an IR services vendor. It is worth noting that more than four in ten (41%) specified that their cyber insurance provider **required** them to purchase an IR service retainer.



**84%**

of organizations currently utilize **cyber insurance** as a risk mitigation strategy.

Impact cyber insurance providers have had on IR strategies.






BACK TO CONTENTS

# IR Service Acquisition Challenges

As organizations work to engage IR service providers, challenges exist. With increasingly more IR service options available, determining the best fit for a specific organization's needs can be overwhelming and confusing. And this choice is often ultra-time-critical, especially for those without retained services. In the middle of a ransomware attack, every minute counts, so spending time comparing and contrasting IR service provider options is not an option. This highlights the importance of preparing in advance of a crisis. Beyond these challenges, organizations with weak or no IR plans are often challenged to work together across IT, security, and line-of-business units.

Challenges acquiring IR services.

**40%**
Overwhelmed and confused by choices of different service providers and options

**38%**
The urgency of the situation forced us to make a quick decision without a proper selection process

**34%**
Lack of or confusion in leadership/ownership of the engagement process

**29%**
Lack of cross-departmental cooperation

**28%**
Pushback due to expectations that IR could be handled internally

**26%**
Low priority compared with other security investments

**25%**
Lack of program maturity

**22%**
Lack of funding



BACK TO CONTENTS

# Urgency Exists in IR Preparedness, Driving Increased Investment

# Urgency Exists in IR Preparedness, Driving Increased Investment and Pursuit of New Providers

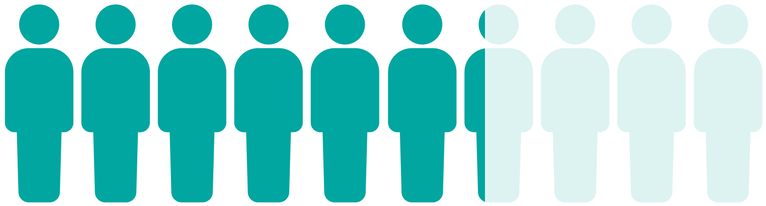
With no end in sight for successful cyber attacks, it's not a question of if, but a question of when and how ready organizations are. Additionally, while confidence levels in detection and response capabilities are generally high, 43% reported that these activities took longer than they should have. Given all these factors, it's no surprise that more than half (51%) plan to significantly increase investment in IR service providers in the coming 12-18 months, with another 37% slightly increasing investment. Additionally, nearly two-thirds (62%) are actively in pursuit of an IR service provider, as the realization of the importance of IR preparedness is recognized.

Rating ability to quickly detect and respond to cybersecurity incidents before they cause significant adverse business impact.

- We have had instances where detection and response took too long, **40%**
- We have had **many** instances where detection and response took too long, **3%**

Will your organization increase spending with incident response service providers in the next 12 to 18 months?

- Yes, significantly **51%**
- Yes, somewhat **37%**



**62%**

of organizations are **actively in pursuit** of a new IR service provider.



BACK TO CONTENTS

FORTRA®

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.

Discover more about Fortra's Alert Logic managed security services, including Extended Detection and Response (XDR), Managed Detection and Response (MDR), and Managed Web Application Firewall (WAF) at alertlogic.com.

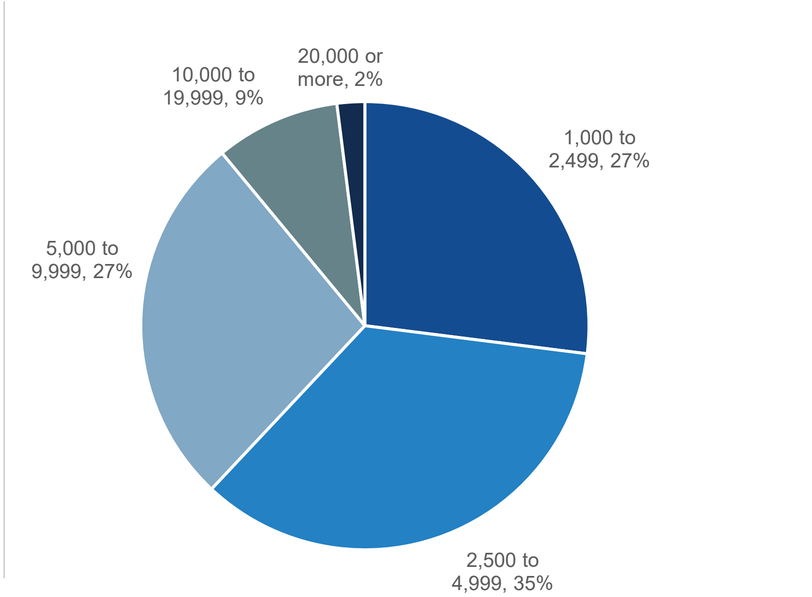
**Learn more**

# Research Methodology and Demographics

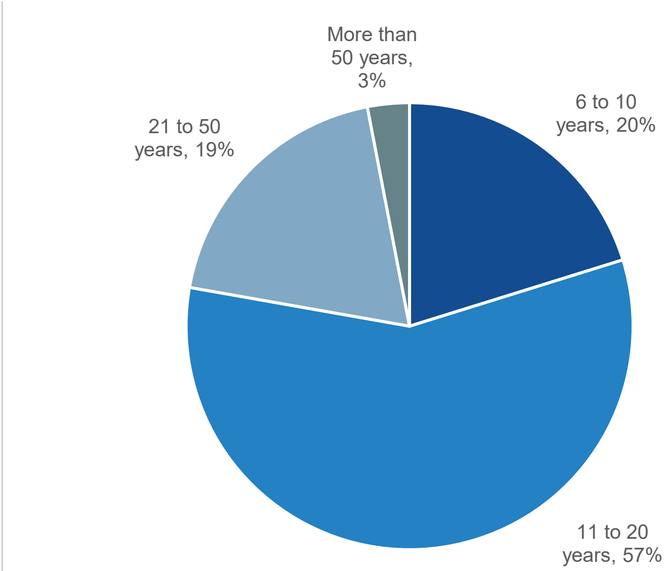
To gather data for this report, TechTarget's Enterprise Strategy Group conducted a comprehensive online survey of cybersecurity professionals from private- and public-sector organizations in North America between October 26, 2022 and November 6, 2022. To qualify for this survey, respondents were required to be cybersecurity professionals with knowledge of and participation in their organization's cyber-threat intelligence programs. 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 380 cybersecurity professionals.

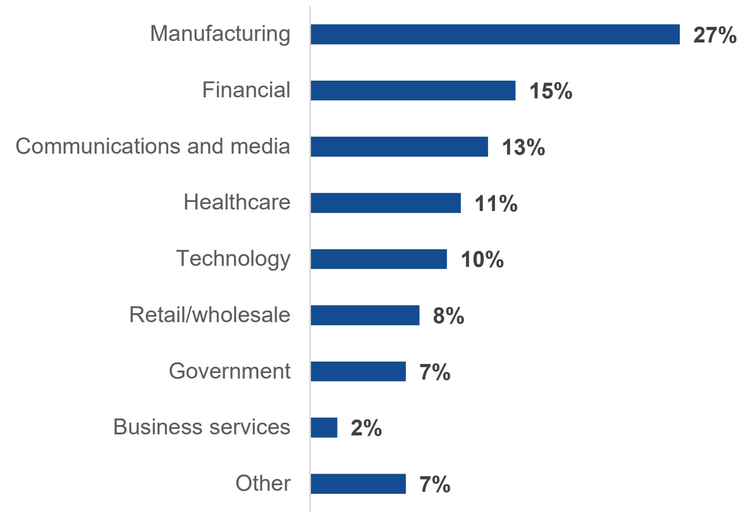
RESPONDENTS BY NUMBER OF EMPLOYEES.




RESPONDENTS BY AGE OF ORGANIZATION.




RESPONDENTS BY INDUSTRY.






BACK TO CONTENTS


**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.