2022

Cybersecurity
INSIDERS

MANAGED SECURITY REPORT

INTRODUCTION

Most IT and security professionals agree that while security is critically important for their organization, they're still facing major challenges to effectively managing it in-house. Managed security services have emerged as a practical, cost-effective option to close the cybersecurity staffing and competency gap and improve organizations' overall security posture. The 2022 Managed Security Report reveals current challenges and illustrates why and how organizations invest in managed security services. It also provides insights into the security capabilities that companies are prioritizing.

Key findings include:

- A majority of organizations operate their security programs primarily in-house (56%). About a quarter of companies follow a hybrid approach of in-house and outsourced resources (23%). Fifteen percent of organizations outsource all of their security operations.
- The perennial shortage of in-house cybersecurity skills (47%) continues to top the list of security operations challenges. This issue is followed by the lack of 24/7 security coverage (38%) and the cost and complexity of building in-house security operations (37%).
- To respond to incoming cybersecurity threats, less than a third of organizations (28%) confirm they can only perform ad-hoc monitoring with IT professionals as the need arises. About one-quarter of organizations (23%) have a team for responding to security incidents when they occur. About another quarter (23%) performs 24/7 monitoring and orchestration of threat detection, analysis and response.

We hope you'll find this report informative and helpful as you continue your efforts in securing your organizations against evolving threats.

Thank you,

Holger Schulze

Holger Schulze
CEO and Founder
Cybersecurity Insiders

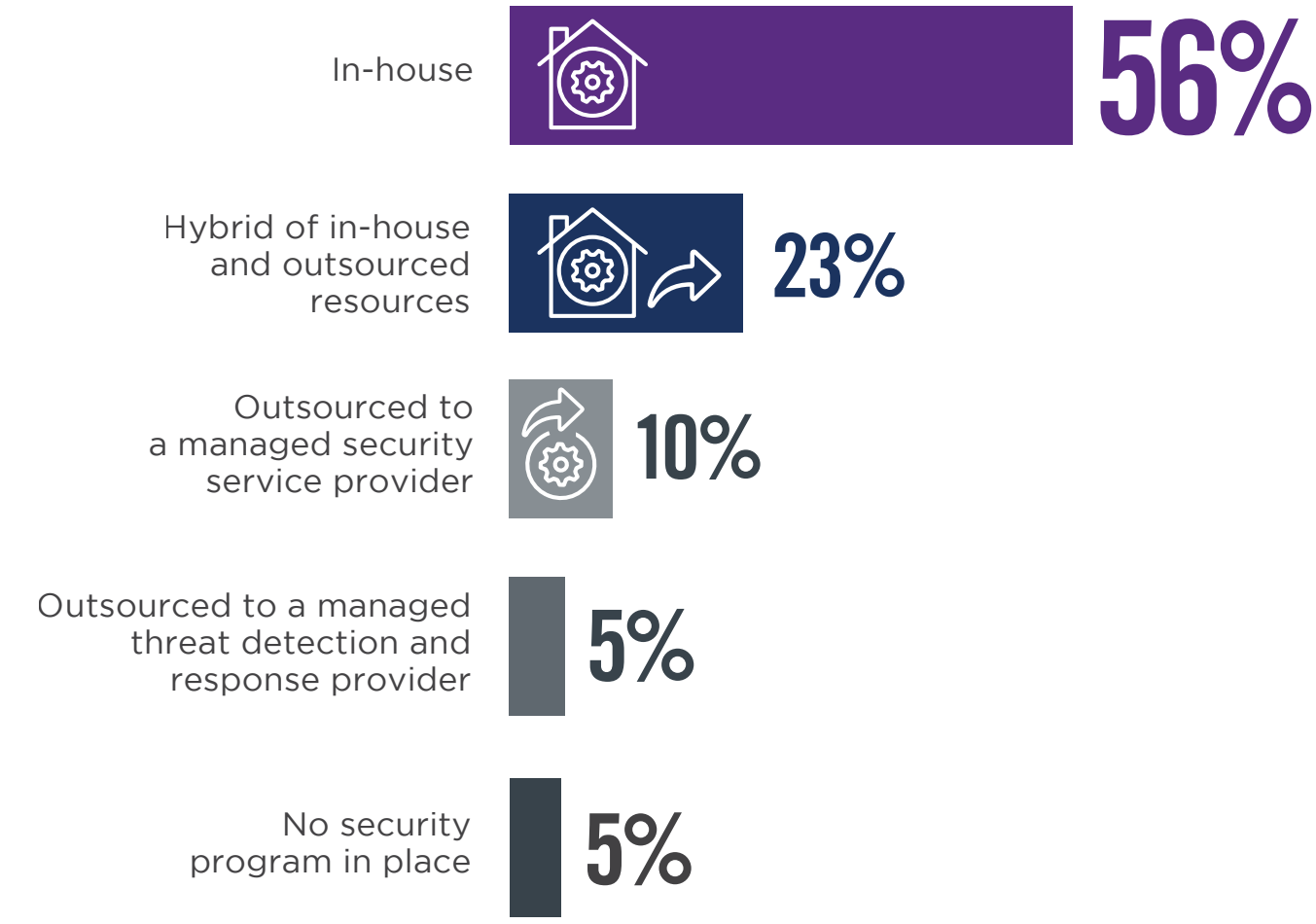
Cybersecurity
INSIDERS

Copyright © 2022 Cybersecurity Insiders. All Rights Reserved.

SECURITY OPERATIONS SOURCING

While the trend toward managed services is gaining momentum, a majority of organizations operate their security programs primarily in-house (56%). About a quarter of companies follow a hybrid approach of in-house and outsourced resources (23%). Fifteen percent of organizations outsource all of their security operations.

How is your security operations program currently sourced?



Other 1%

Copyright © 2022 Cybersecurity Insiders. All Rights Reserved.

SECURITY OPERATIONS CHALLENGES

When asked about the top security operations challenges facing their IT organization, the perennial shortage of in-house cybersecurity skills continues to top the list (47%). This issue is followed by the lack of 24/7 security coverage (38%) and the cost and complexity of building in-house security operations (37%). These challenges are the exact same issues managed security services are designed to address.

What are the top three security operations challenges for your IT organization?

47%

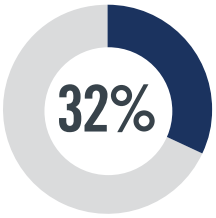
Cybersecurity skills shortage in-house

38%

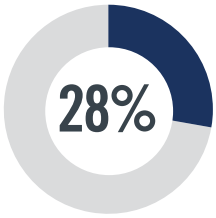
Lack of 24/7 security coverage

37%

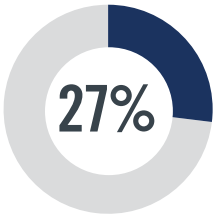
Cost and complexity of building in-house



Speed of incident response issues



No visibility into overall security posture



Lack of detection and response capabilities

Speed of deployment and provisioning issues 26% | Lack of customization of correlation rules and reports 19% | Not able to meet compliance requirements 17% | Getting adequate budget approved 14% | Can't effectively deal with cloud security 6% | Other 8%

Copyright © 2022 Cybersecurity Insiders. All Rights Reserved.

THREAT PREPAREDNESS

We asked cybersecurity professionals how equipped their staff and processes are to deal with incoming threats. While respondents have varying levels of threat monitoring and response capacity, as much as 13% have no skilled security analysts or incident response personnel in-house. Less than a third of organizations (28%) confirm they can only perform ad-hoc monitoring with IT professionals as the need arises. About one-quarter of organizations (23%) have a team for responding to security incidents when they occur. About another quarter (23%) performs 24/7 monitoring and orchestration of threat detection, analysis and response.

How equipped are your staff and processes to deal with incoming threats?

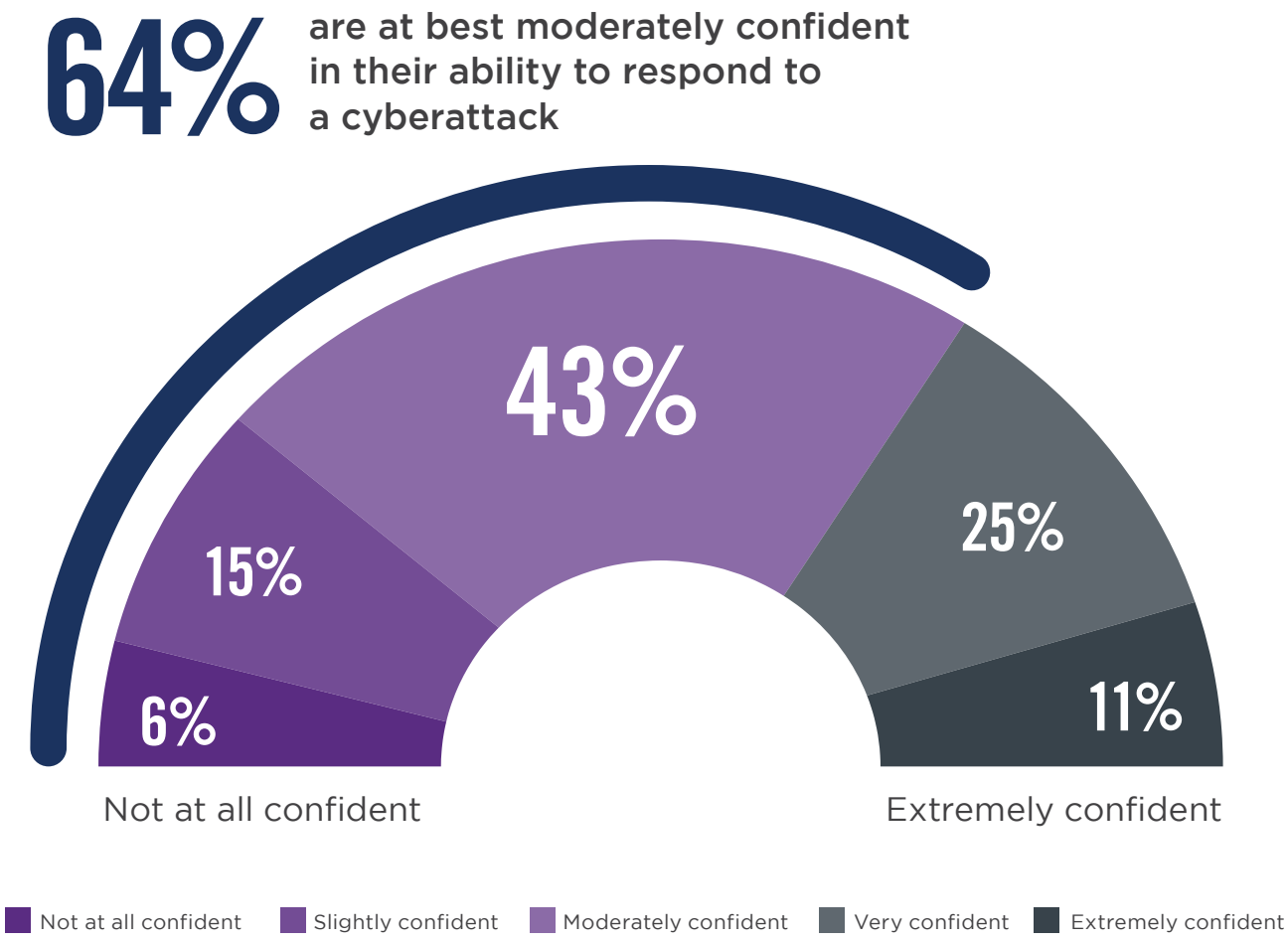
Other 2%

Copyright © 2022 Cybersecurity Insiders. All Rights Reserved.

ATTACK RESPONSE CONFIDENCE

The majority of survey respondents (64%) are at best only moderately confident in their ability to respond to a cyberattack. This finding confirms other industry research which shows that there is a pressing need for robust, 24/7 security threat detection and response.

How confident are you in your organization's ability to respond to a cyberattack?



Copyright © 2022 Cybersecurity Insiders. All Rights Reserved.

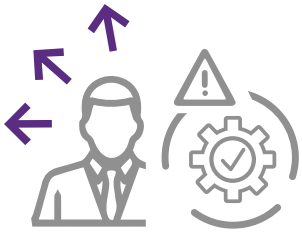
SECURITY INCIDENT IMPACT

Security incidents cause a variety of disruptions to organizations. The biggest negative impact of security incidents is disrupted business activities (38%). This is followed by the deployment of IT resources necessary to triage and remediate security issues (33%) and reduced employee productivity (31%).

What negative impacts have security incidents had on your company in the past 12 months?

38%

Disrupted business activities

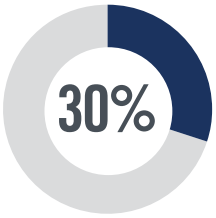


33%

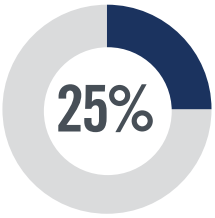
Deployment of IT resources to triage and remediate issue

31%

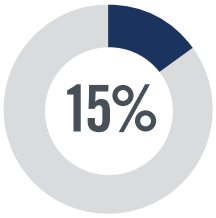
Reduced employee productivity



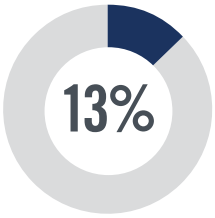
Not applicable/ we haven't had any incidents



Increased helpdesk time to repair damage



Reduced revenue/ lost business



Corporate data loss or theft

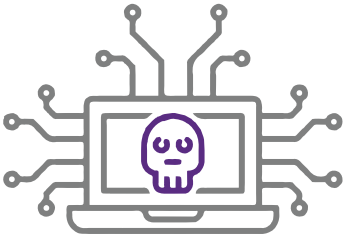
Loss/compromise of intellectual property 12% | Regulatory fines 8% | Lawsuit/legal issues 8% | Other 4%

Copyright © 2022 Cybersecurity Insiders. All Rights Reserved.

RISK OF COMPROMISE

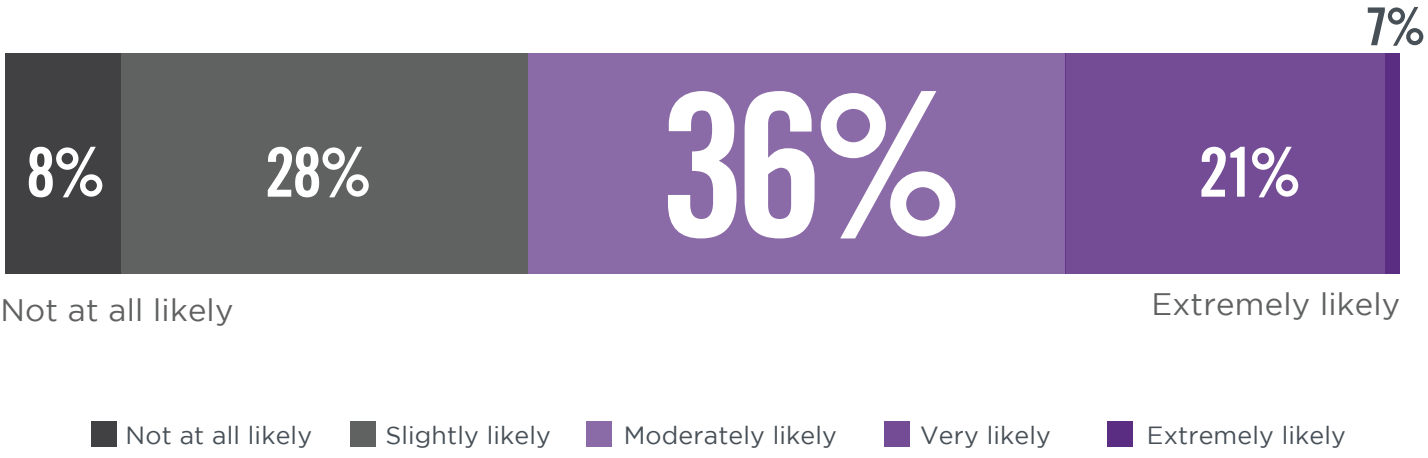
We asked cybersecurity professionals about the likelihood that their organization will become compromised by a successful cyberattack in the next 12 months. A majority of respondents (64%) see it as moderately to extremely likely that their organization will be affected by a successful cyberattack.

What do you believe is the likelihood that your organization will become compromised by a successful cyberattack in the next 12 months?



64%

consider it at least moderately likely that their organization will be compromised by a successful cyberattack in the next 12 months



Copyright © 2022 Cybersecurity Insiders. All Rights Reserved.

RELIANCE ON FRAMEWORKS

To what degree are organization relying on standard security frameworks, customized to their industry, for their security operations? Unfortunately, only about a third rely on a standard security framework (31%) and take advantage of the benefits of proven cybersecurity operations models.

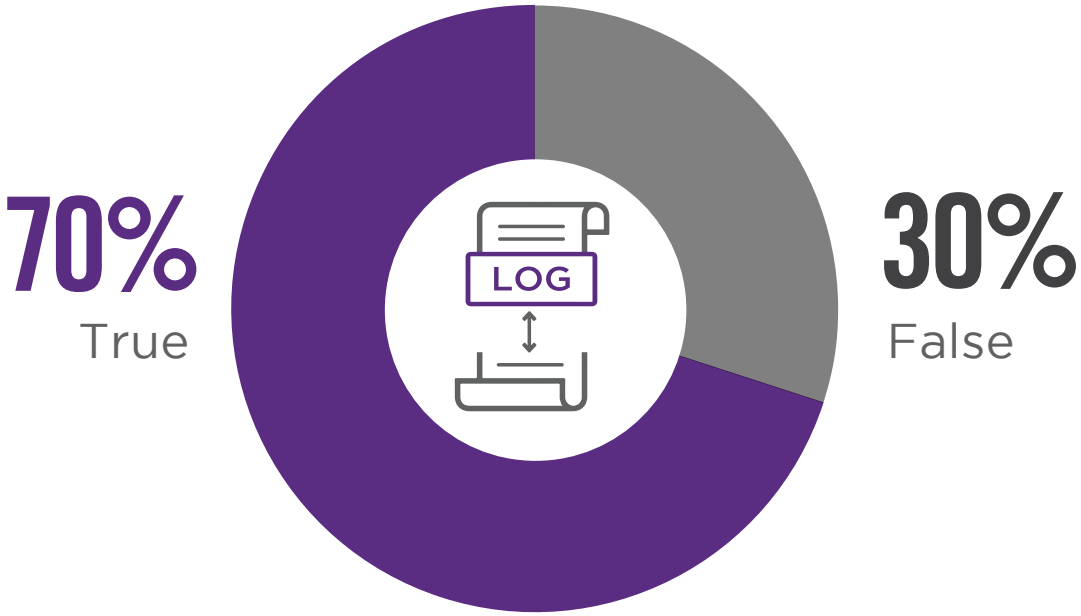
My organization's existing security plan is built on a standard security framework and is customized to my industry.

Copyright © 2022 Cybersecurity Insiders. All Rights Reserved.

AREAS OF OPPORTUNITY

Seventy percent of security professionals see areas of opportunity in their threat detection capabilities.

I have identified log source coverage gaps and areas of opportunity in my organization's threat detection capabilities



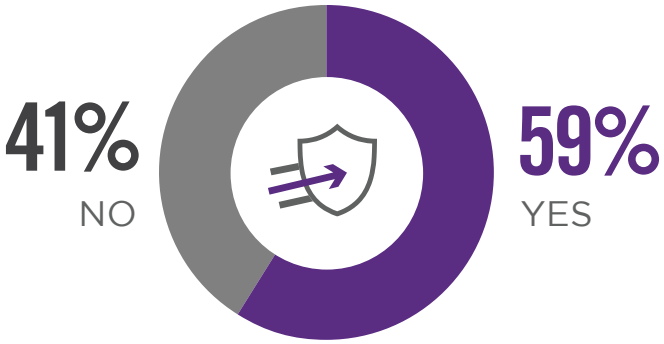
Copyright © 2022 Cybersecurity Insiders. All Rights Reserved.

INSIDER RISK

We asked survey participants how prepared their organizations are to protect against insider attacks. Of organizations surveyed, 52% confirm they don't have enough security resources in-house to contain or deter insider threats. Forty-one percent of teams do not perform an annual penetration test or implement red team operations to test their security controls. Sixty-nine percent of security professionals are at most moderately confident that they are strong enough to prevent an insider attack.

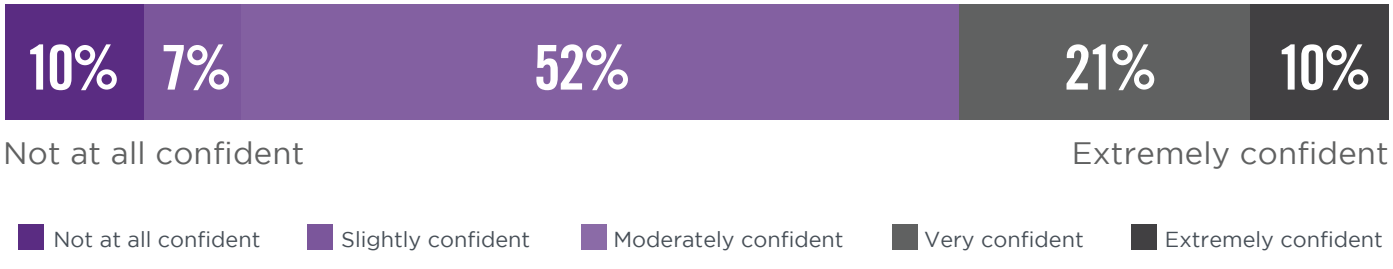
Do you have enough security resources in-house to contain or deter insider threats?

I perform at minimum an annual penetration test and red team operations to test my security controls



How confident are you that your security awareness programs are strong enough to prevent insider threat (e.g., phishing)?

69% of security professionals are not at all to moderately confident they are strong enough to prevent an insider attack

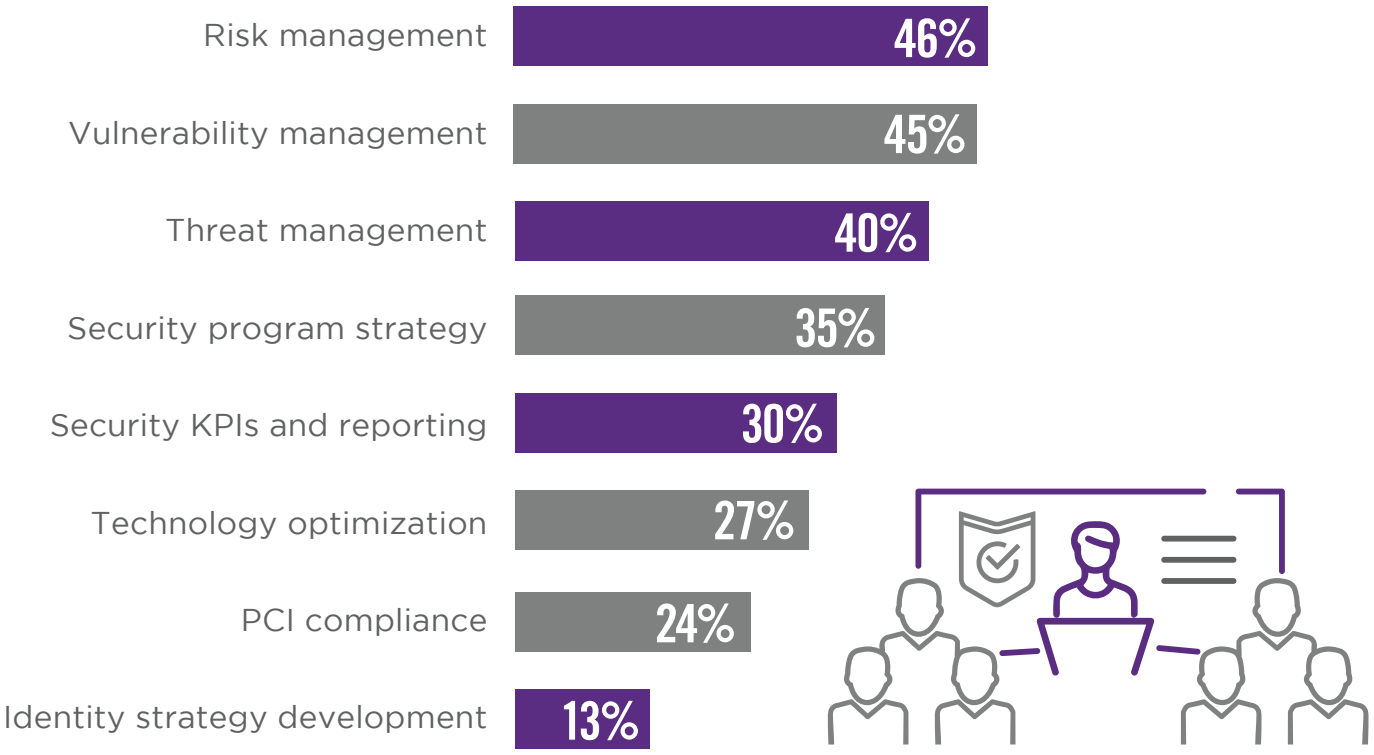


Copyright © 2022 Cybersecurity Insiders. All Rights Reserved.

SECURITY WORKSHOP FOCUS

Security workshops are a popular method to assess security capabilities. Organizations report that their workshops prioritize overall risk management (46%), followed by vulnerability management (45%) and threat management (40%).

Have you held a security workshop with your internal team to assess your capabilities in at least one of the following areas in the past 12 months?



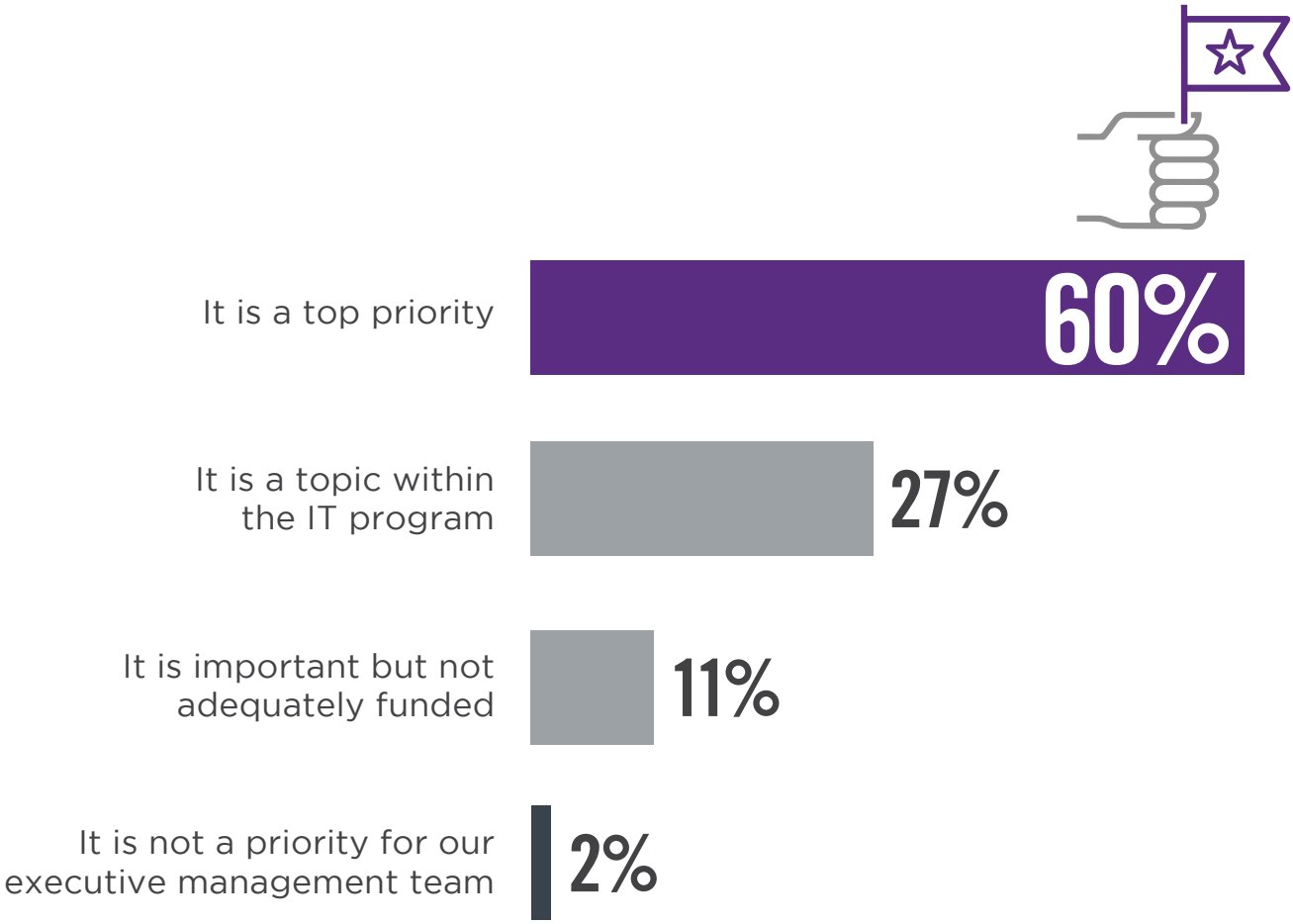
None of the above 25% | Other 2%

Copyright © 2022 Cybersecurity Insiders. All Rights Reserved.

IMPORTANCE OF SECURITY

More than half of cybersecurity professionals (60%) confirm that security is a top priority for their organization. However, organizations still face significant hurdles and challenges towards implementing their security objectives.

How important is security to your organization?



Copyright © 2022 Cybersecurity Insiders. All Rights Reserved.

WHY USE AN MSSP?

Why do organizations increasingly rely on managed security service providers? The top three reasons include the ability to rapidly respond to security incidents (44%), followed by a lack of internal security personnel/expertise (42%) and potential cost savings (42%).

If you're NOT currently using a Managed Security Service Provider, what would drive you to do so?

44%

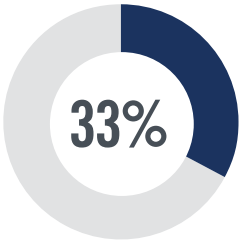
Ability to respond to incidents

42%

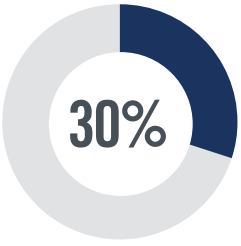
Lack of internal security personnel/expertise

42%

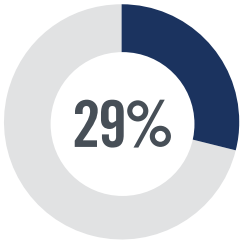
Potential cost savings



Meeting regulatory compliance mandates



Board/executive level concern over our breach potential



A breach event at our organization

Customer/partner demand 17% | Deploying new cloud applications and infrastructure 13% | Mergers and acquisition activity 10% | Other 10%

Copyright © 2022 Cybersecurity Insiders. All Rights Reserved.

MSSP SELECTION CRITERIA

When selecting a Managed Security Services Provider (MSSP), organizations prioritize 24/7 security coverage above all else (61%). This is followed by the total cost of the MDR solution (55%) and the ability to integrate and leverage existing security technology stacks (48%).

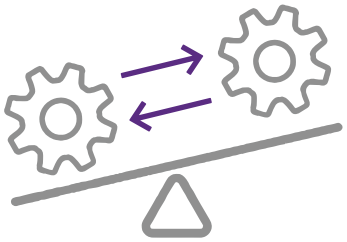
What are the top 3 factors that are most important to you when selecting a managed detection and response provider?

61%

24/7 coverage of security operations

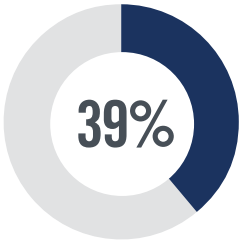
55%

Solution cost

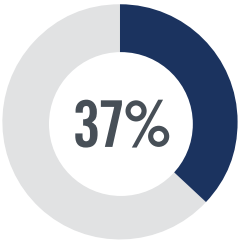


48%

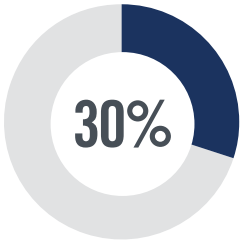
Ability to integrate/ leverage our security technology stack



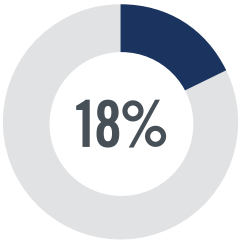
Supported systems or technologies



Reputation of company and leadership



Ability to customize reporting



Location/proximity (ability to interact with a local or regional analyst)

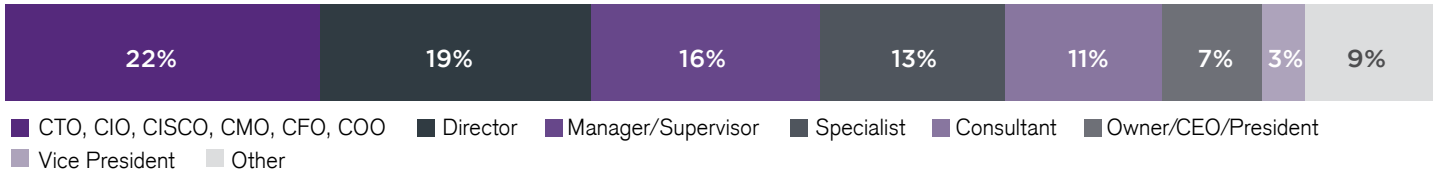
Complete solution with consulting services (professional services including incident response, pen testing, etc.) 15% | Ability to easily see what MSSP analysts see at any time and what activity has been performed 14% | Ability to support cloud applications and infrastructure security 11% | Personalized customer service 10% | Other 3%

Copyright © 2022 Cybersecurity Insiders. All Rights Reserved.

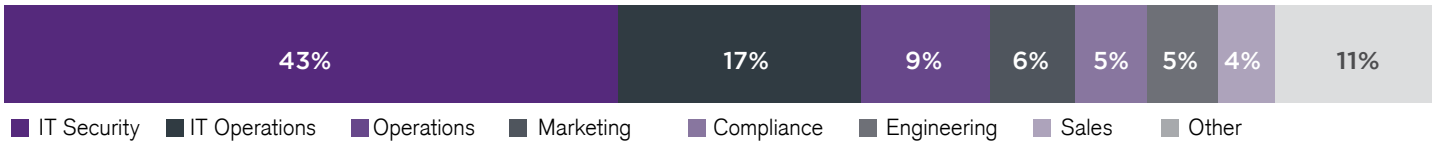
METHODOLOGY & DEMOGRAPHICS

This report is based on the results of a comprehensive online survey of IT and cybersecurity professionals conducted in 2022. It reveals the latest trends and attitudes toward managed security, answering why organizations invest in security outsourcing, what challenges they are facing, and what requirements companies are prioritizing. The respondents range from technical executives to senior managers and IT security practitioners, across the spectrum of company sizes and industries, representing a balanced cross-section of organizations.

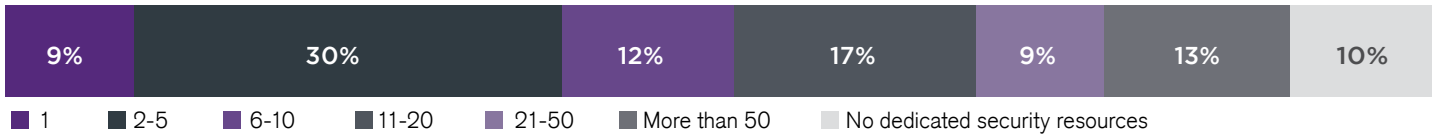
CAREER LEVEL



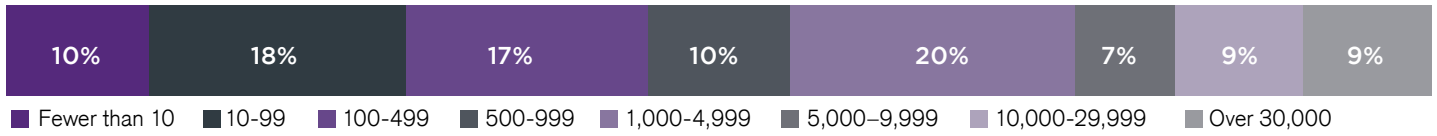
DEPARTMENT



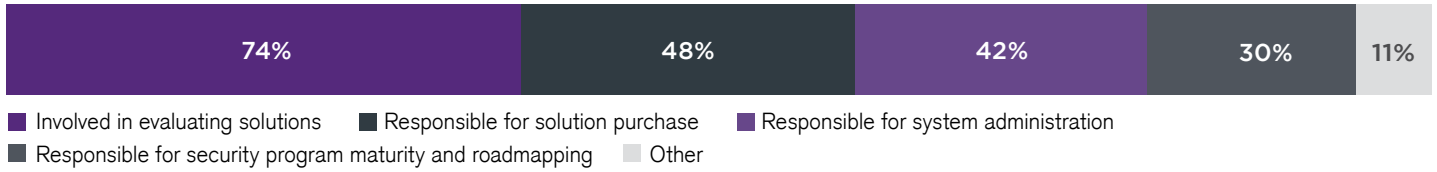
IT SECURITY TEAM HEADCOUNT



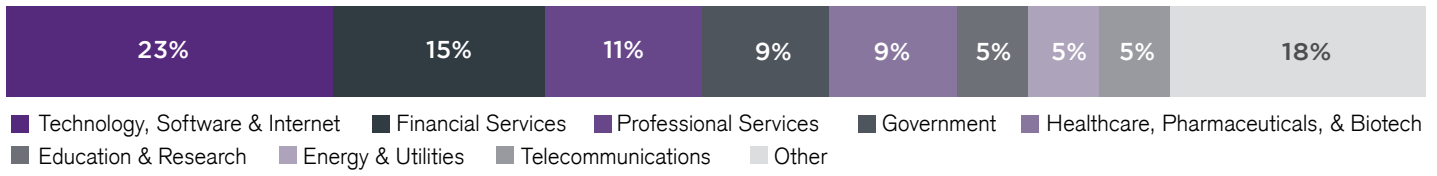
COMPANY SIZE



LEVEL OF INVOLVEMENT IN SECURITY



INDUSTRY



Copyright © 2022 Cybersecurity Insiders. All Rights Reserved.

Cybersecurity INSIDERS

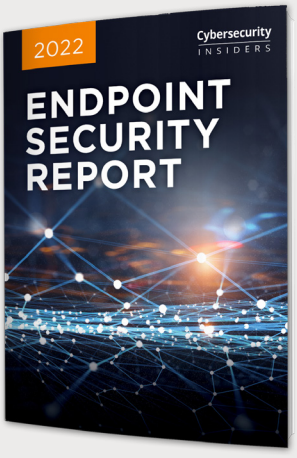
Cybersecurity Insiders is a 500,000+ member online community for information security professionals, bringing together the best minds dedicated to advancing cybersecurity and protecting organizations across all industries, company sizes, and security roles.

We provide cybersecurity marketers with unique marketing opportunities to reach this qualified audience and deliver fact-based, third-party validation thought leadership content, demand-generation programs, and brand visibility in the cybersecurity market.

Interested in seeing your brand featured in the next report?

Contact Cybersecurity Insiders for more information at: **info@cybersecurity-insiders.com**

- FACT-BASED CONTENT
- SALES-READY LEADS
- BRAND AWARENESS



For more information please visit www.cybersecurity-insiders.com

All Rights Reserved. ©2022 Cybersecurity Insiders. Data can be reproduced or referenced as long as it is sourced and linked to www.cybersecurity-insiders.com.