2020

Cybersecurity
INSIDERS

STATE OF MANAGED SECURITY REPORT

DELTA RISK

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 2020 State of 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 confirm that security programs are still primarily operated in-house (54%). This is followed by a quarter of organizations (25%) that use a hybrid of in-house and outsourced resources, and a smaller number of organizations that outsource all of their security operations (8%).
- The top three security operations challenges include the perennial shortage of cybersecurity skills in-house (51%), followed by the cost and complexity of building in-house security operations (38%), tied with the lack of continuous 24x7 security coverage (38%).
- To respond to incoming cybersecurity threats, less than a third of organizations (27%) can only perform ad-hoc monitoring with IT professionals as the need arises. About one-quarter (24%) of respondents say they have a team for responding to security incidents when they occur, but they do not perform continuous monitoring.

We would like to thank Delta Risk for supporting this important industry research project. 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

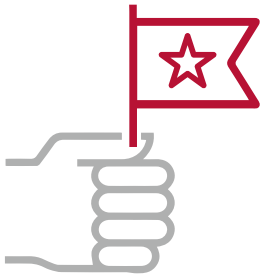
Holger Schulze
CEO and Founder
Cybersecurity Insiders

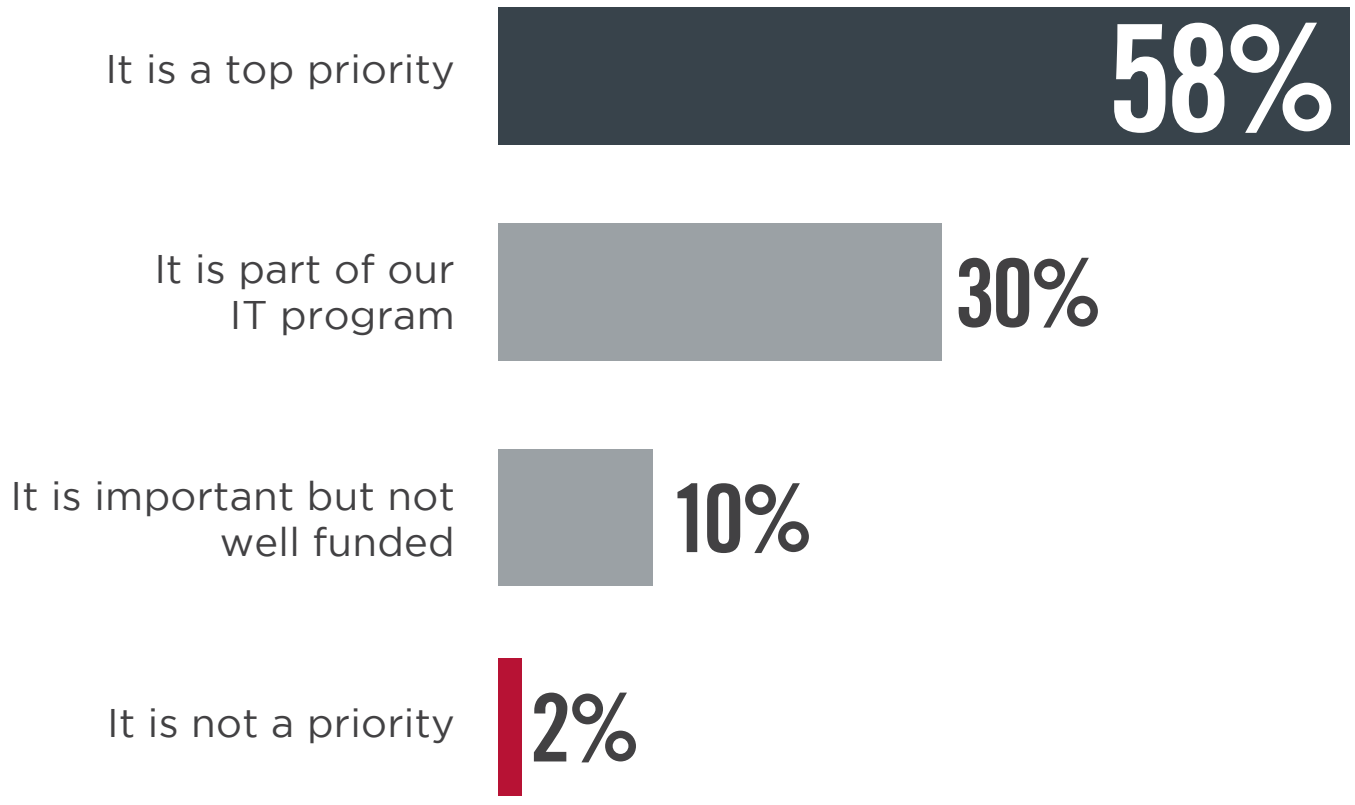
Cybersecurity
INSIDERS

IMPORTANCE OF SECURITY

More than half of organizations confirm that security is a top priority (58%). However, the following survey results reveal that organizations still face significant hurdles and challenges towards implementing their security objectives.

Is security a priority in your organization?

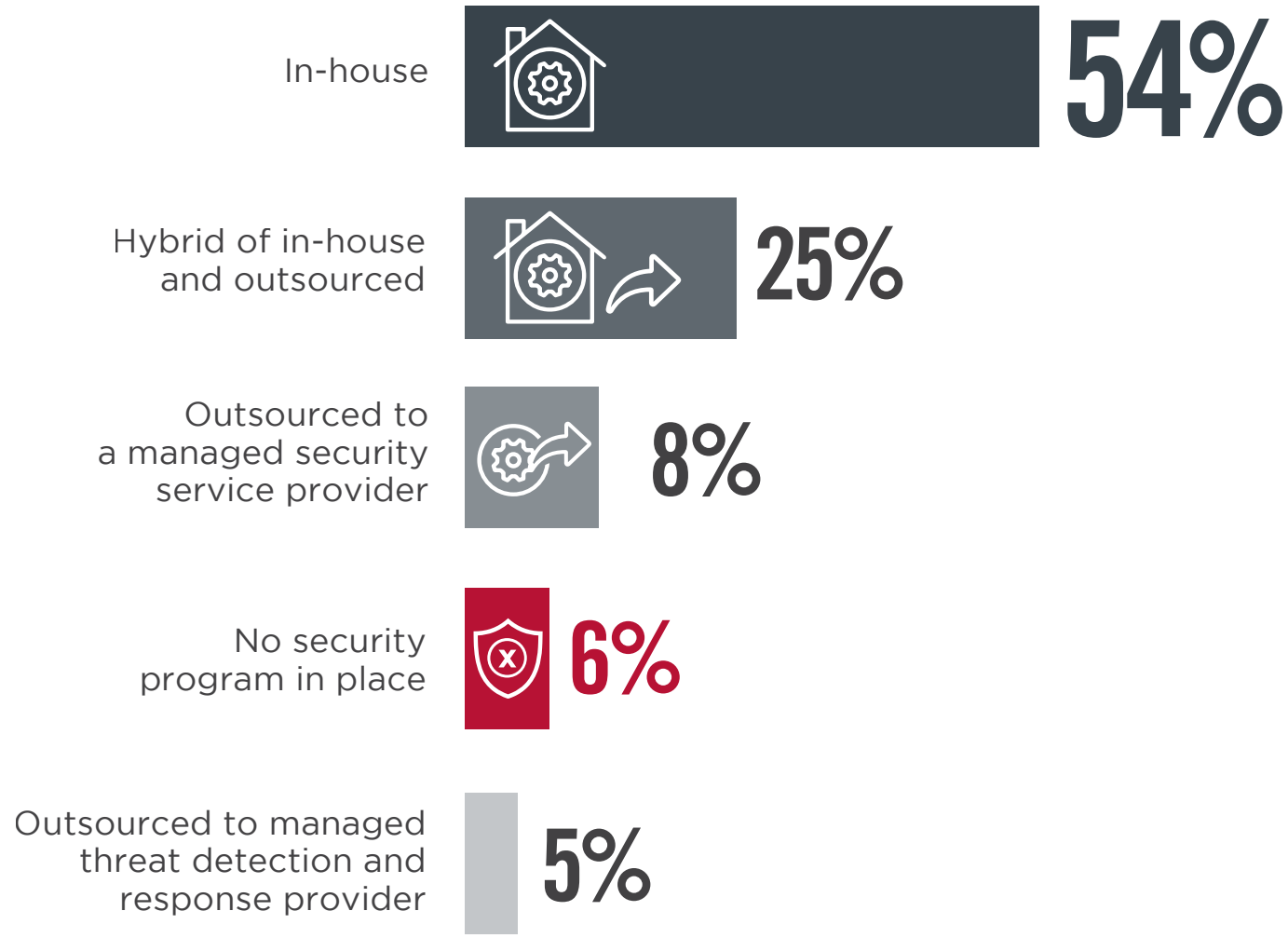




SECURITY OPERATIONS SOURCING

A majority of organizations confirm that their security programs are primarily operated in-house (54%). This is followed by a quarter of organizations (25%) who operate in a hybrid fashion of in-house and outsourced resources, and organizations who outsource all of their security operations (8%).

How is your security operations program currently sourced?



Other 2%

SECURITY OPERATIONS CHALLENGES

The top three security operations challenges experienced by IT organizations include the perennial shortage of cybersecurity skills in-house (51%), followed by the cost and complexity of building in-house security operations (38%), tied with the lack of continuous 24x7 security coverage (38%). These are the exact same issues managed security services are designed to address.

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

51%

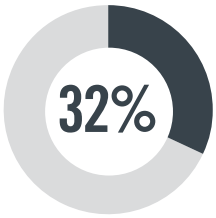
Cybersecurity skills shortage in-house

38%

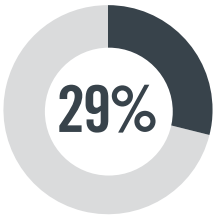
Cost and complexity of building in-house

38%

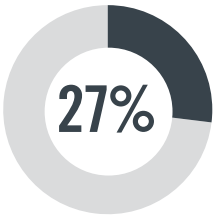
Lack of 24x7 security coverage



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%

THREAT PREPAREDNESS

To respond to incoming cybersecurity threats, less than a third of organizations (27%) confirm they can only perform ad-hoc monitoring with IT professionals as the need arises. About one-quarter (24%) of respondents say they have a team for responding to security incidents when they occur, but they do not perform continuous monitoring. Only 23% have a dedicated security operations center (SOC) in place that monitors and orchestrates threat analysis and response centrally, and continuously tests and hones processes for optimal end-to-end threat lifecycle management.

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

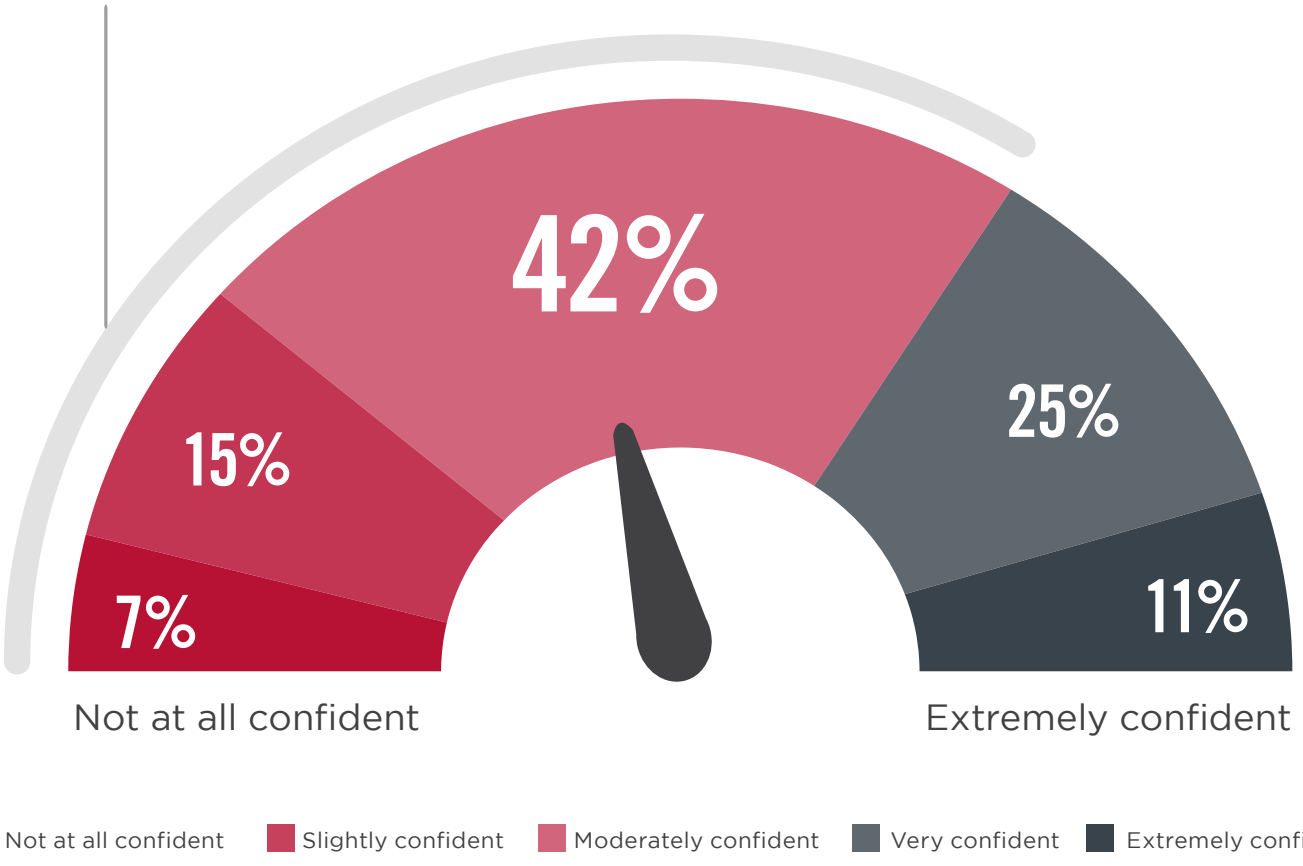
Other 1%

ATTACK RESPONSE CONFIDENCE

The majority of respondents (64%) are moderately confident (or less) in their ability to respond to a cyberattack. This finding coincides with other recent industry research to show that there is an overall need for dedicated, 24x7 security threat detection and response.

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

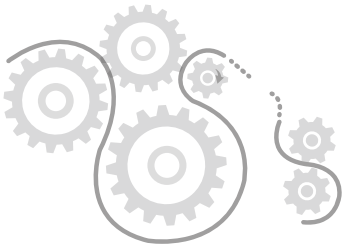
64% Are at best moderately confident in their ability to respond to a cyberattack.



SECURITY INCIDENT IMPACT

The biggest negative impact companies are reporting from security incidents stems from disrupted business activities (37%), followed by reduced employee productivity (32%) which is tied with the deployment of IT resources to triage and remediate security issues (32%).

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



37%

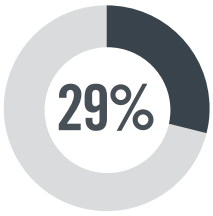
Disrupted business activities

32%

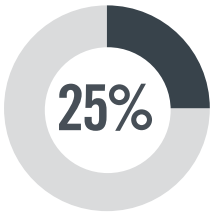
Reduced employee productivity

32%

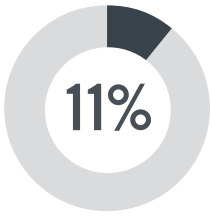
Deployment of IT resources to triage and remediate issue



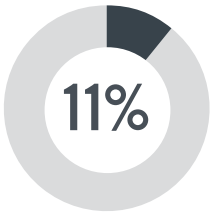
Not applicable/ we haven't had any incidents



Increased helpdesk time to repair damage



Reduced revenue/ lost business



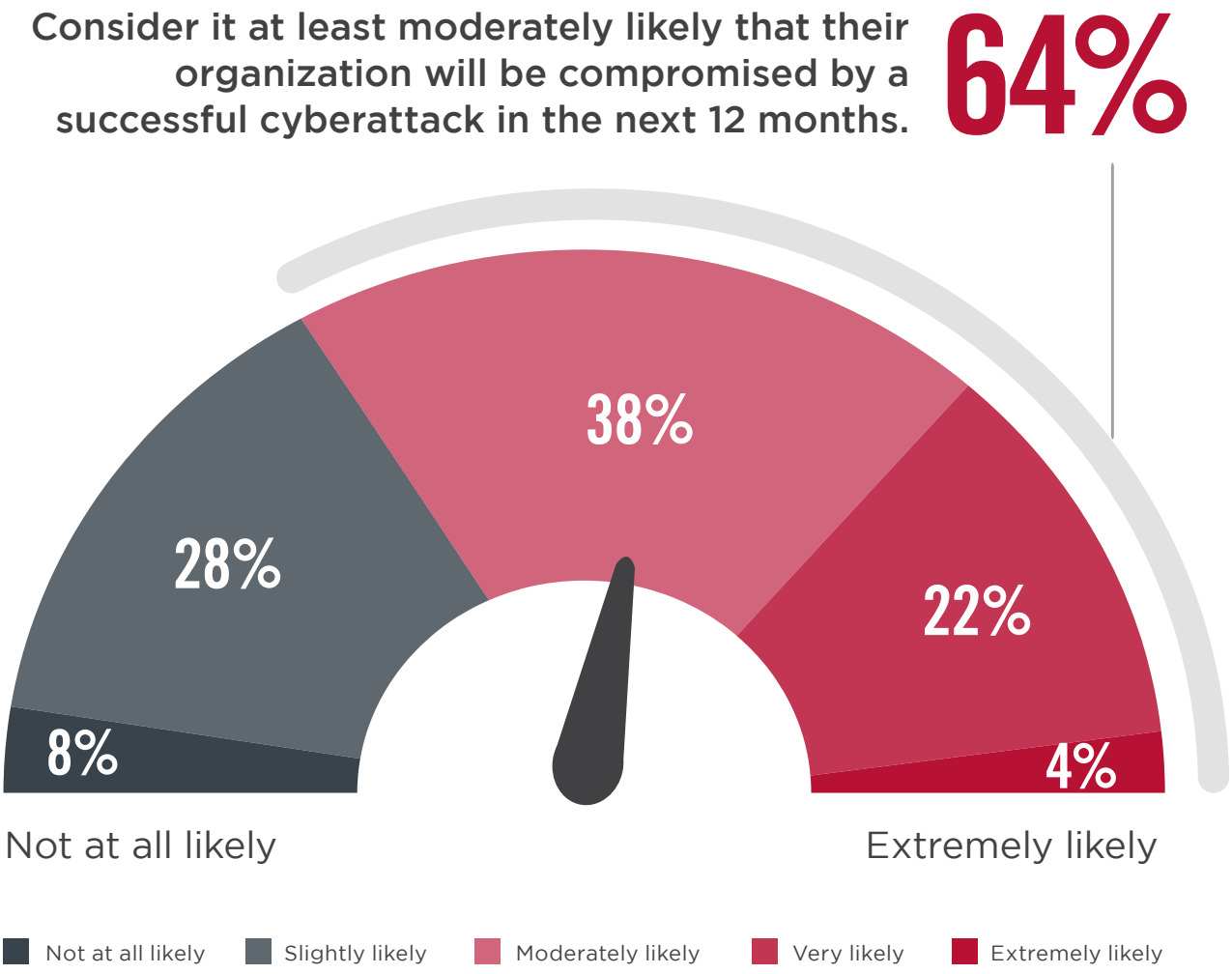
Loss/compromise of intellectual property

Corporate data loss or theft 10% | Regulatory fines 8% | Lawsuit/legal issues 7% | Other 5%

RISK OF COMPROMISE

A majority (64%) are concerned that their organization will be compromised by a successful cyberattack in the next 12 months.

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

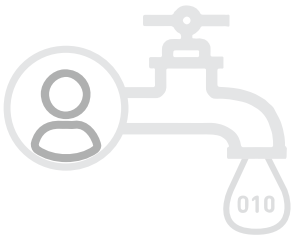


KEY THREATS

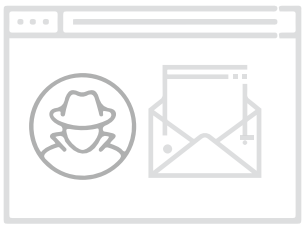
Of all the cyber threats facing organizations, ransomware (73%) is most concerning. This is followed by loss of customer data (57%) and email account compromise (39%).

What are the most concerning threats to your organization?

73% Ransomware



57%
Loss of customer data



39%
Email account compromise

36%
Compliance findings/fines

Other 4%

WHY USE MANAGED SECURITY SERVICES

We asked organizations not currently using managed security services what factors would change their mind. These include a lack of internal security personnel/expertise (43%), the desired ability to better respond to security incidents (42%), closely followed by potential cost savings (41%).

If you're NOT currently using a managed security service provider, what would drive you to sign up for a managed service?

43%

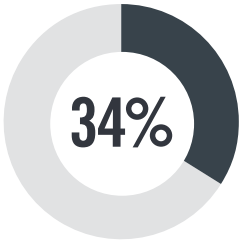
Lack of internal security personnel/expertise

42%

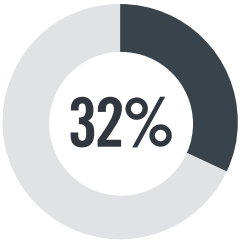
Ability to respond to incidents

41%

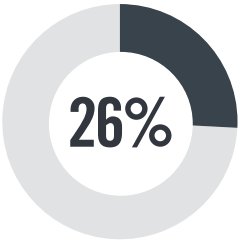
Potential cost savings



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 10% | Mergers and acquisition activity 6% Other 10%

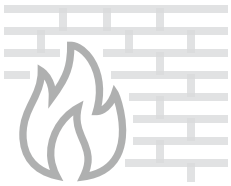
MOST IMPORTANT SECURITY SERVICES

We asked organizations to rank managed security services in order of importance. The service considered most critical is managed detection and response, followed by managed SIEM and firewall management.

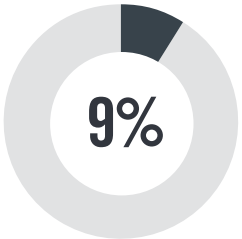
What are the most important managed security services to your company?

26%
Managed detection and response

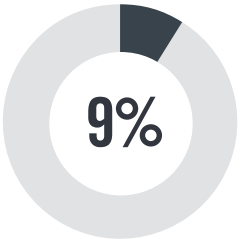
25%
Managed SIEM



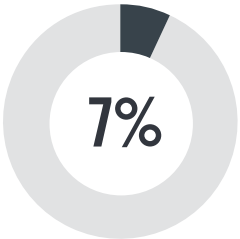
14%
Firewall management



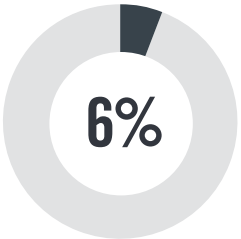
Endpoint management



Security assessment and/or penetration testing



Compliance consulting and/or auditing



Vulnerability scanning

Security Orchestration Automation and Response (SOAR) 4% | Advanced threat intelligence 4% | Cloud application security 4% | Cloud infrastructure security 4% | Managed phishing 2%

SERVICE PROVIDER SELECTION

When selecting a Managed Security Services Provider (MSSP), organizations prioritize 24/7 security coverage above all else (63%). This is followed by the cost of the MDR solution (54%) and the ability to integrate and leverage their existing security technology stack (50%).

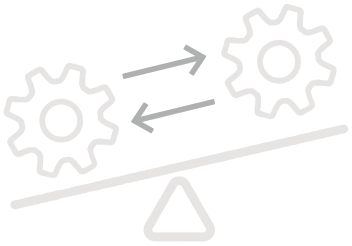
What are the top 3 factors that are most important to you when selecting a managed detection and response provider?

63%

24/7 coverage of security operations

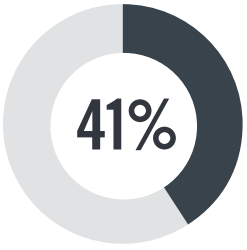
54%

Solution cost

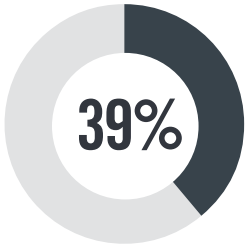


50%

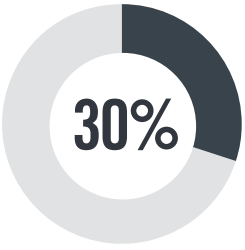
Ability to integrate/ leverage our security technology stack



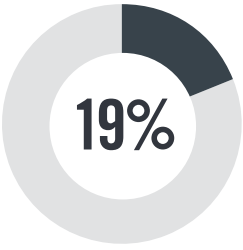
Supported systems or technologies



Reputation of company and leadership



Ability to customize reporting



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

Ability to easily see what MSSP analysts see at any time and what activity has been performed 10% | Complete solution with consulting services (professional services including incident response, pen testing, etc.) 9% | Ability to support cloud applications and infrastructure security 8% | Personalized customer service 5% | Other 4%

MANAGED SECURITY BUDGETS

For 42% of organizations, budgets allocated to managed security services are expected to increase. Only 14% expect a decline.

How will your budget for outsourced managed security change over the next 12 months?

42%
Budget will increase

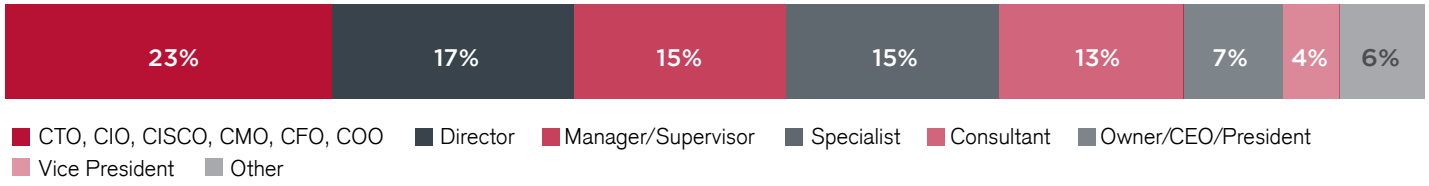
44%
Budget will stay the same

14%
Budget will decrease

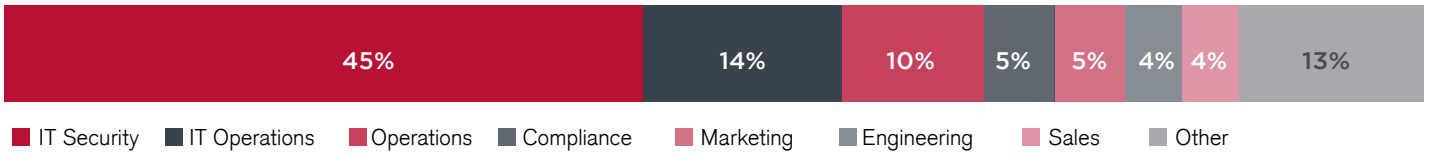
METHODOLOGY & DEMOGRAPHICS

This report is based on the results of a comprehensive online survey of 317 IT and cybersecurity professionals conducted in April 2020. 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.

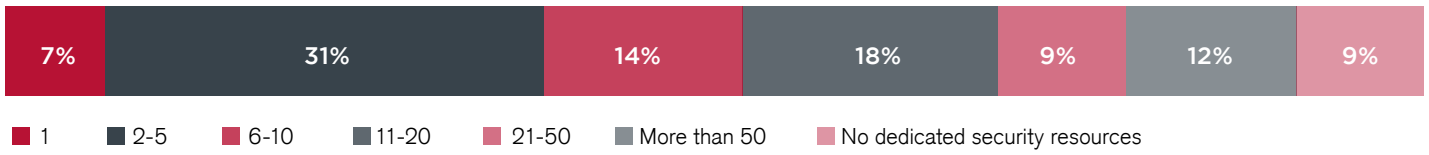
CAREER LEVEL



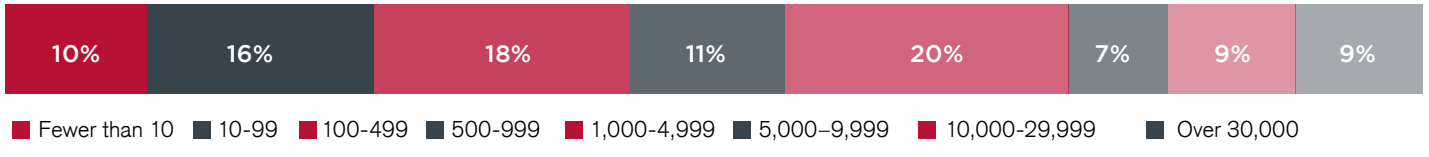
DEPARTMENT



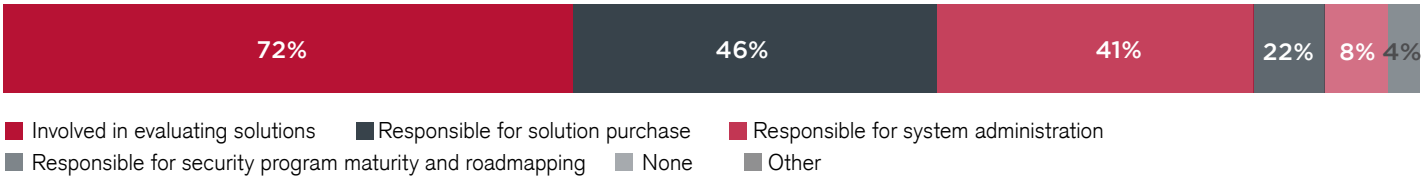
IT SECURITY TEAM HEADCOUNT



COMPANY SIZE



LEVEL OF INVOLVEMENT IN SECURITY



Delta Risk is breaking the mold for managed security, delivering Security Operations Center (SOC)-as-a-Service and security services that bridge the gap to a modern security approach. We enable any size organization to leverage our expert security operations team and respond to endpoint, network, and cloud security threats 24/7. ActiveEye, our proprietary platform, uses Security Orchestration Automation and Response (SOAR) to cut through the noise and address the most critical threats faster. The ActiveEye Portal is the cornerstone of our customer-centric approach, providing clients a transparent view into SOC activities and Key Performance Indicators (KPIs) that demonstrate the value of our co-managed security approach.

www.deltarisk.com