HERJAVEC GROUP

Managed Security Services Trends

2020

Cybersecurity INSIDERS

Introduction

Herjavec Group, a global leader in cybersecurity operations, has partnered with Cybersecurity Insiders to produce the Managed Security Services Trends 2020. This report summarizes the results of a comprehensive survey of 400,000 information security professionals and aims to highlight the challenges and considerations that organizations have when it comes to Managed Security Services Providers (MSSP).

The results here reflect the opinions of IT security decision makers from a variety of industries including, but not limited to, Software & Technology, Government, Healthcare, Professional Services, Education, and Manufacturing. Most businesses represented in this survey support anywhere from 1,000 to 10,000 network-connected endpoints (servers, laptops, workstations, IOT, printers, etc.).

Ultimately, we all recognize that technology alone cannot prevent today's cyber attacks. Most organizations believe they will likely experience a security incident in the next 6-12 months and acknowledge that quality and speed of response is of utmost concern. The results confirm that internal security teams are challenged to proactively detect and monitor threats 24/7, cutting through the noise of false positives. Many are challenged to keep up with emerging technologies, new threats, and trends. Also, most teams lack internal support or the tools and automation to achieve these objectives.

So where are security leaders prioritizing their security investments?
Where are organizations leveraging third-party service providers to complement their in-house capabilities? What specialized managed services are at the forefront of these offerings?

Read more to learn from your executive peers about the key Managed Security Services considerations for 2020 and check out the important questions you should be asking yourself as an IT business leader.

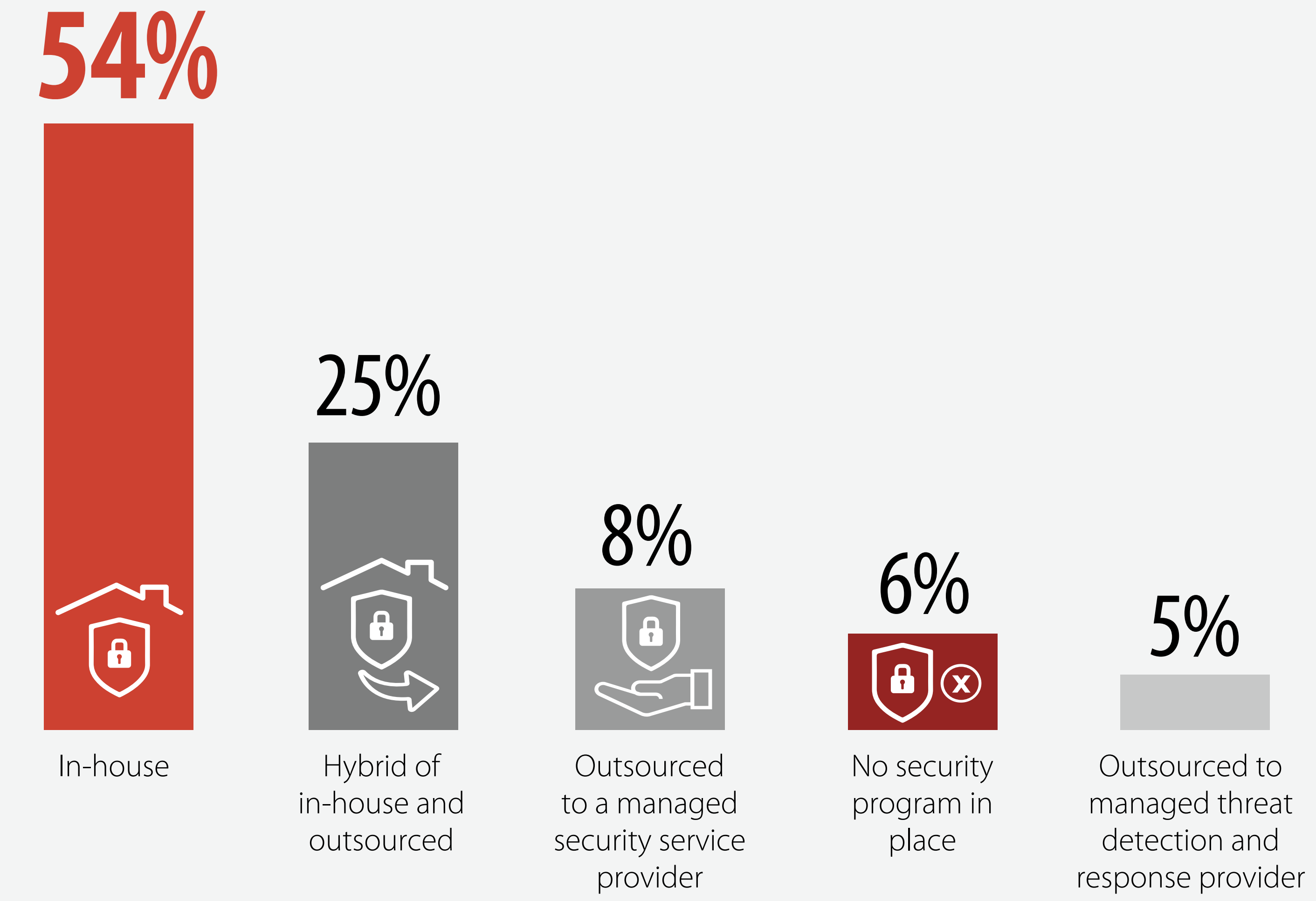
About Herjavec Group

Dynamic IT entrepreneur Robert Herjavec founded Herjavec Group in 2003 to provide cybersecurity products and services to enterprise organizations. We have been recognized as one of the world's most innovative cybersecurity operations leaders, and excel in complex, multi-technology environments. We have expertise in comprehensive security services including Managed Security Services (SOC Operations, Threat Detection, Security Technology Engineering) & Professional Services (Advisory Services, Identity Services, Technology Architecture & Implementation & Incident Response). Herjavec Group has offices and Security Operations Centers across the United States, United Kingdom, India and Canada.

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 continuing 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 issues managed security services are designed to address.

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

51%

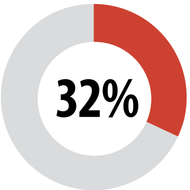
Cybersecurity skills shortage in-house

38%

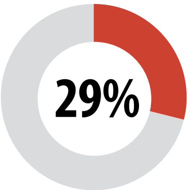
Cost and complexity of building in-house

38%

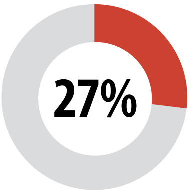
Lack of 24x7 security coverage



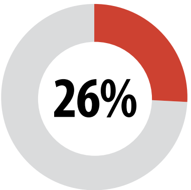
Speed of incident response issues



No visibility into overall security posture



Lack of detection and response capabilities



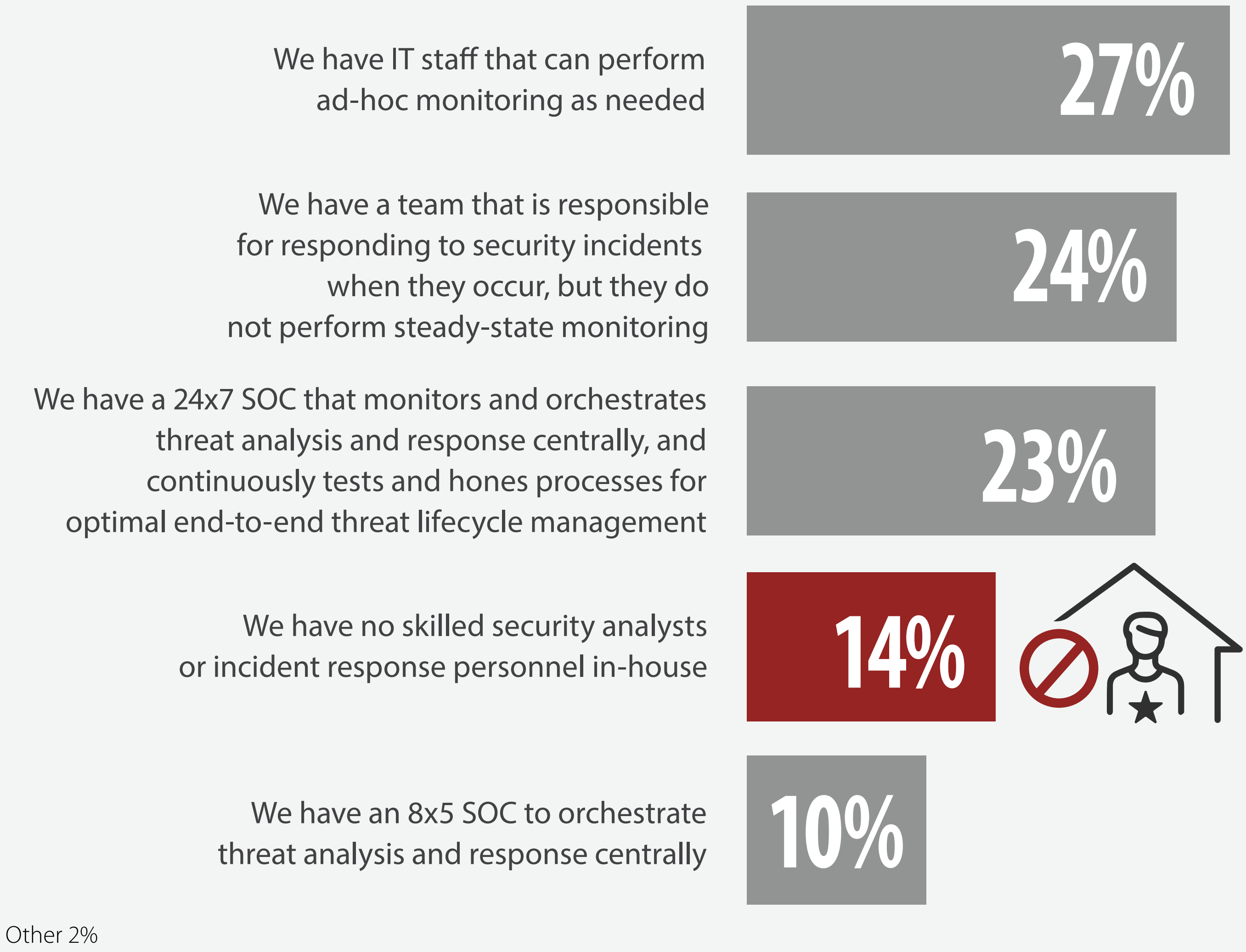
Speed of deployment and provisioning issues

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

Respondents have varying levels of threat monitoring and response coverage, but as much as 14% have no skilled security analysts or incident response personnel in-house. Less than a third of organizations (27%) confirm they can only perform ad-hoc monitoring as the need arises and about one-quarter (24%) have a team for responding to security incidents when they occur, but they do not perform continuous monitoring.

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



Security Incident Impact

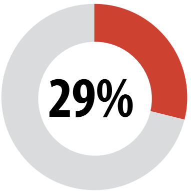
In the past 12 months, 37% of businesses reported disruption to business activities due to security incidents as their biggest negative impact, followed by reduced employee productivity tied with the deployment of IT resources to triage and remediate security issues (32%).

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

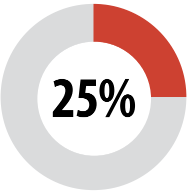
37%
Disrupted business activities

32%
Reduced employee productivity

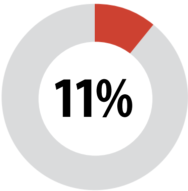
32%
Deployment of IT resources to triage and remediate issue



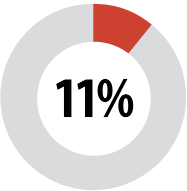
Not applicable/ we haven't had any incidents



Increased helpdesk time to repair damage



Reduced revenue/ lost business



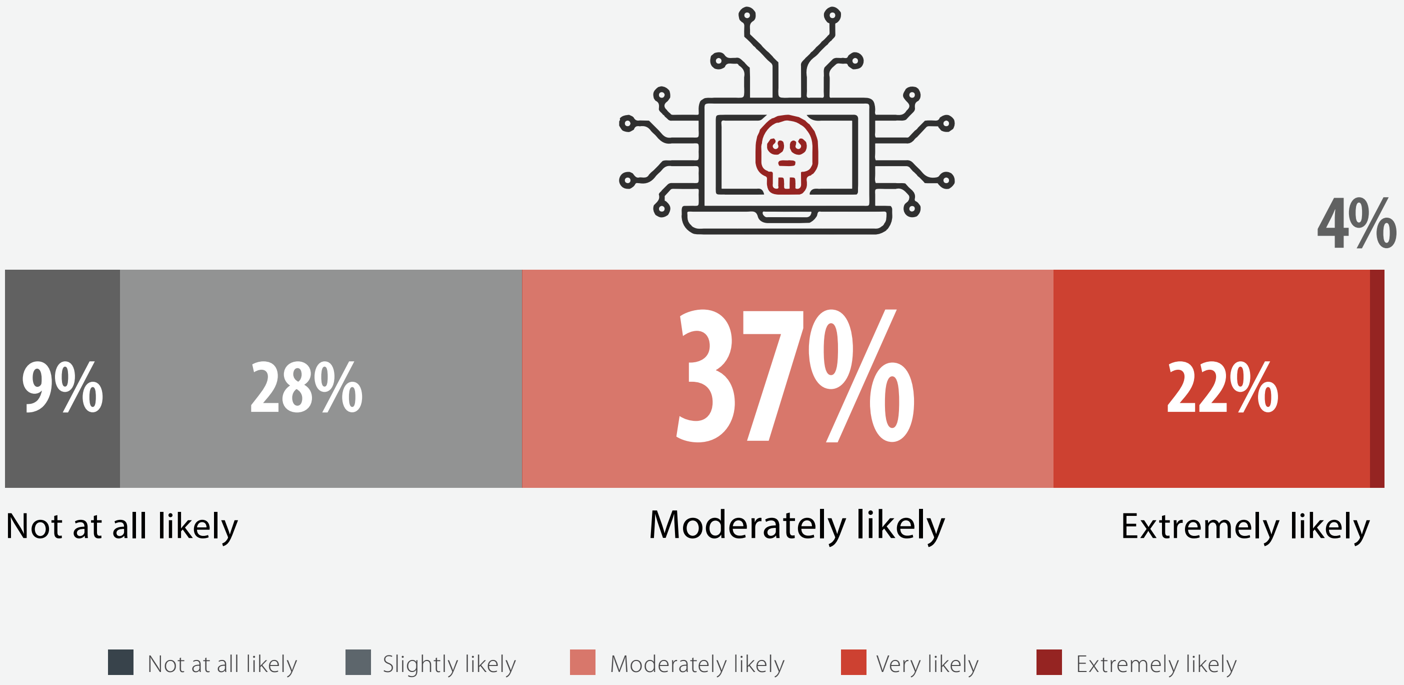
Loss/compromise of intellectual property

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

Risk of Compromise

Thirty-seven percent of businesses think it is moderately likely that their organization will become compromised by a successful cyber attack 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?**



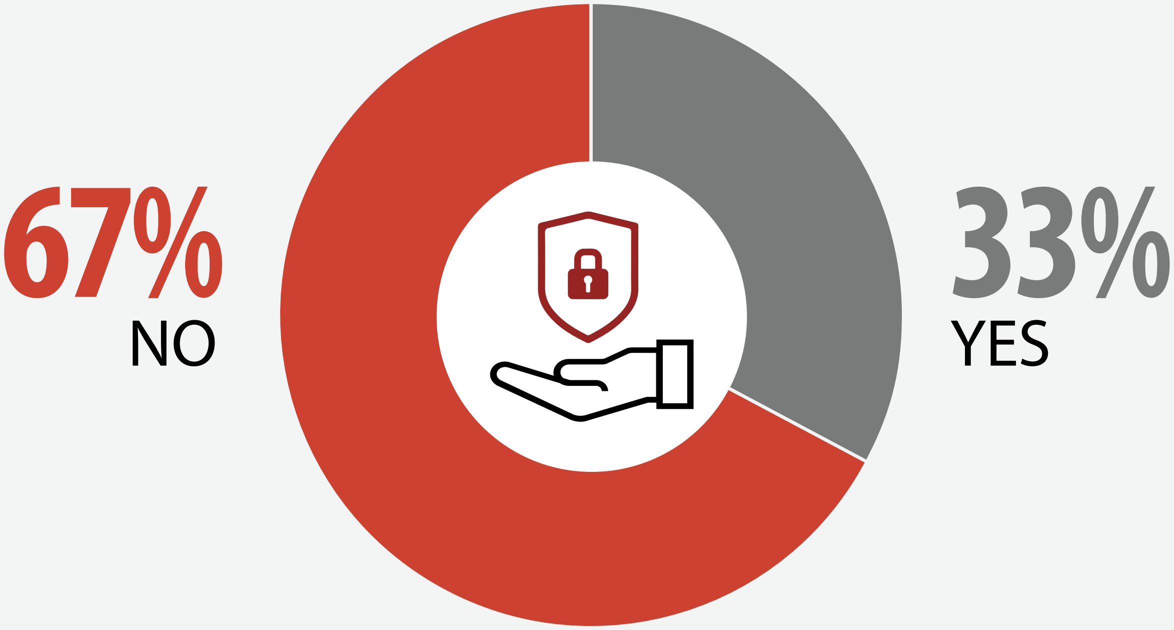
ASK YOURSELF

- □ How does your MSSP use threat management protocols or threat research frameworks?
- □ How does your technology stack fare in terms of its prevention and detection ability?
- □ How strong is your vulnerability management program? Are you utilizing a risk-based approach in how your team prioritizes vulnerabilities?

Identity Governance & Technical Controls

Sixty-seven percent of respondents are not utilizing a Managed Security Service Provider to continuously manage and assess identity governance and technical controls.

▶ Is your company utilizing a Managed Security Service Provider to continuously manage and assess identity governance and technical controls?



☑ ASK YOURSELF

□ What does my current Identity governance plan look like? Do I have the necessary technical controls in place?

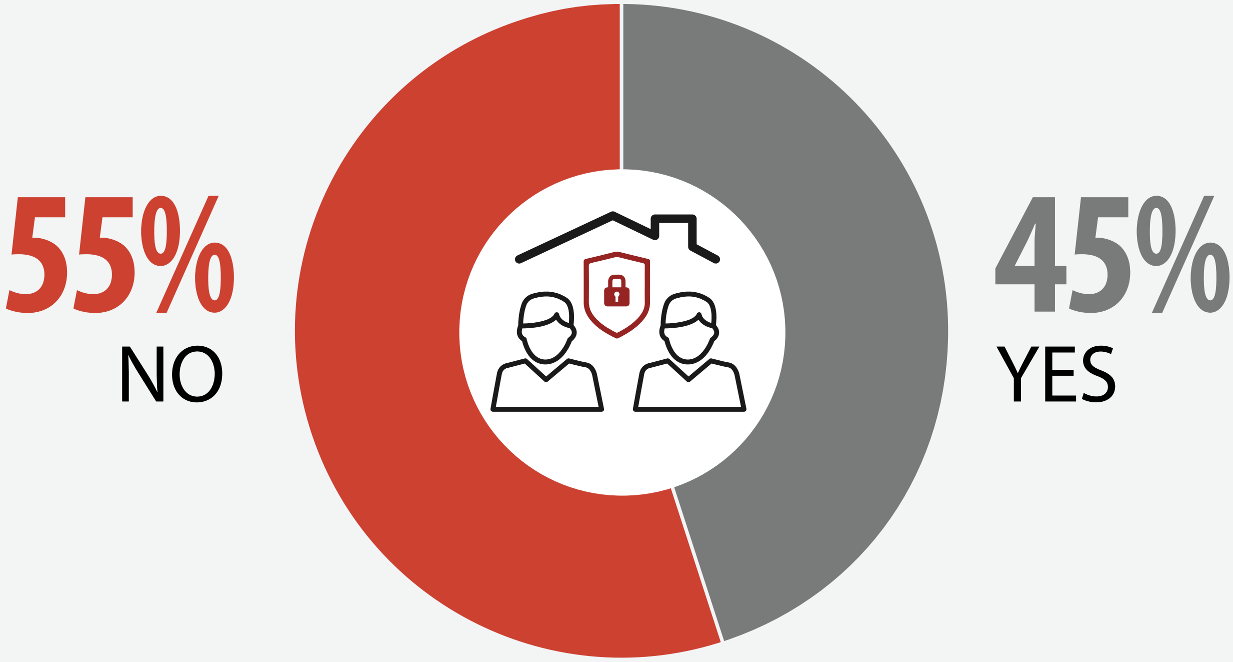
□ When was the last time I assessed my organization's existing Identity program? How have my controls and processes changed since the assessment?

□ Which parts of my identity provisioning and access control process are automated vs manual?

Insider Threat

Today's most damaging security threats do not originate from malicious outsiders or malware, but from trusted insiders with access to sensitive data and systems. Regardless of whether a user is malicious or negligent, insider threat is one of the largest risk to your business. Of organizations surveyed, 55% do not have enough security resources in-house to contain or deter insider threat.

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



☑ ASK YOURSELF

□ Can my organization benefit from Security Orchestration, Automation, and Response (SOAR) technology to account for a lack of in-house resources?

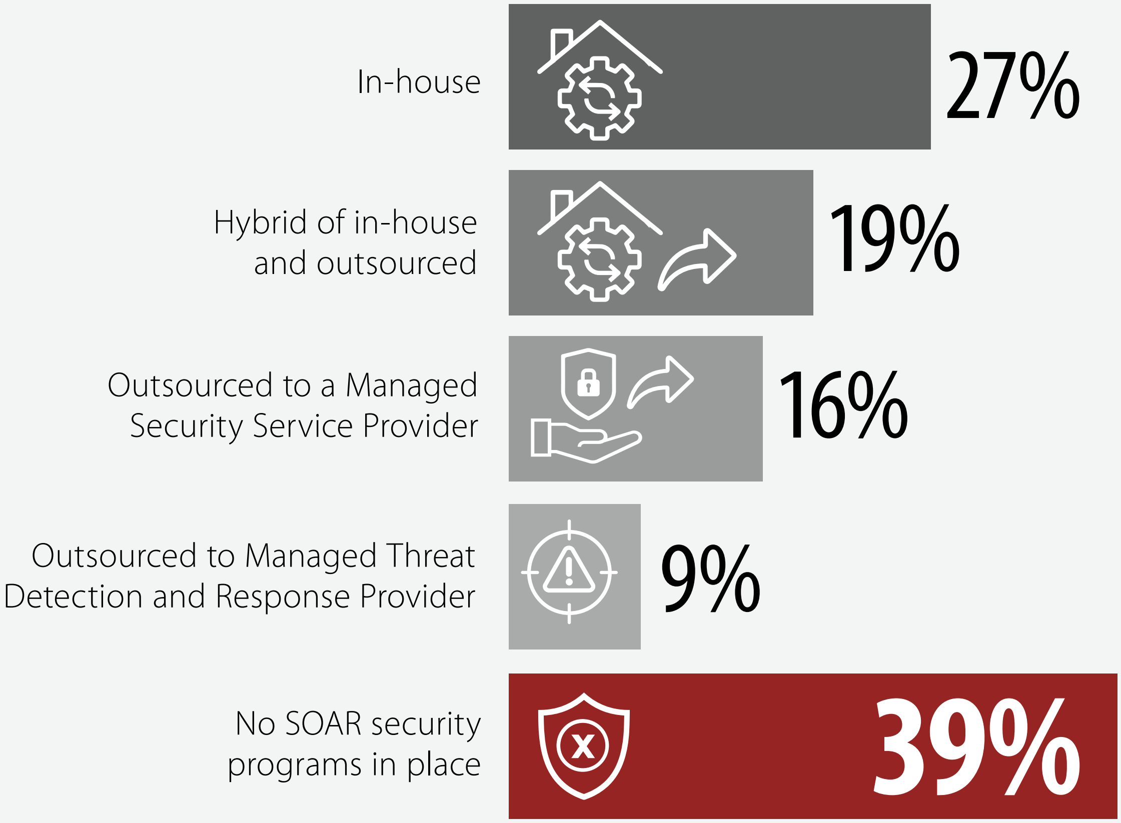
□ Am I leveraging employee security awareness training programs to prevent insider threat?

□ Could my organization benefit from a managed phishing service to support the prevention, detection and remediation of phishing attacks end-to-end?

Security Orchestration Automation and Response (SOAR)

A concerning 39% of respondents are not currently leveraging SOAR. Of the organizations already utilizing Security Orchestration Automation and Response (SOAR), 27% have deployed SOAR in-house, followed by hybrid deployments of in-house platforms and outsourced services (19%).

How are you currently leveraging Security Orchestration Automation and Response (SOAR)?



Other 4%

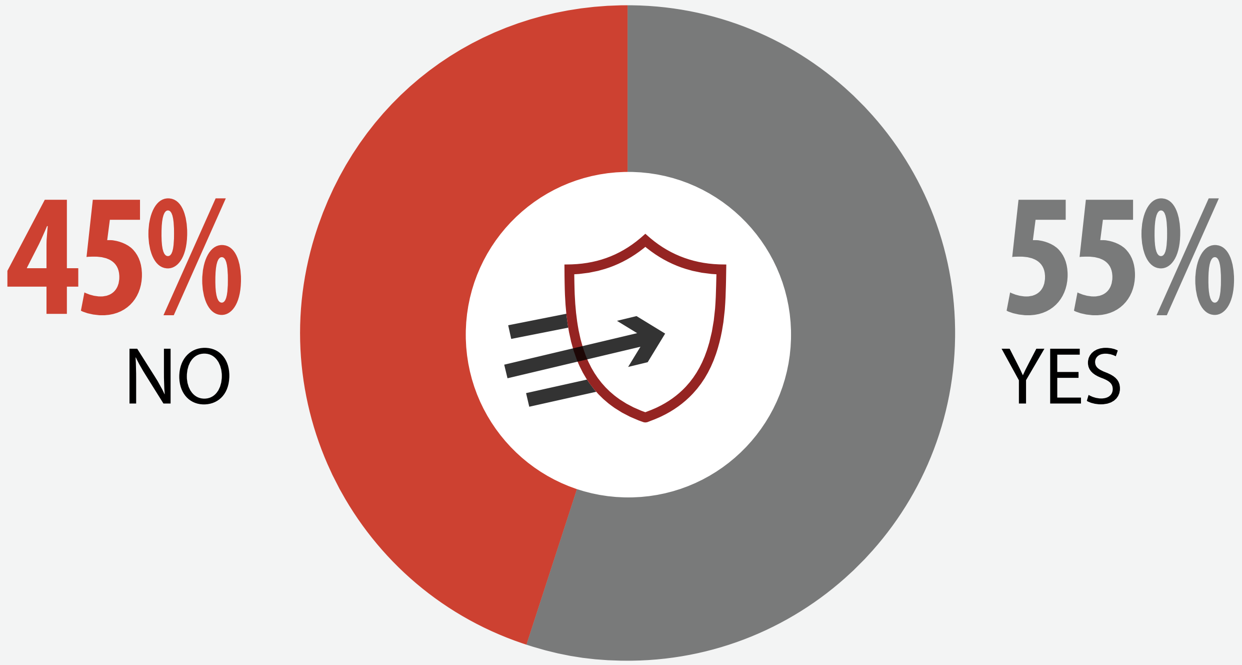
ASK YOURSELF

- □ Is my organization currently considering adopting SOAR technology in-house?
- □ What is my current mean time to detect and mean time to notify for security events?
- □ What tasks are my security analysts doing that could be automated using a SOAR tool?

Security Assessments & Testing

Fourty-five percent of teams do not perform an annual penetration test or red team operations to test their security controls.

Do you perform at minimum an annual penetration test and red team operations to check security controls?



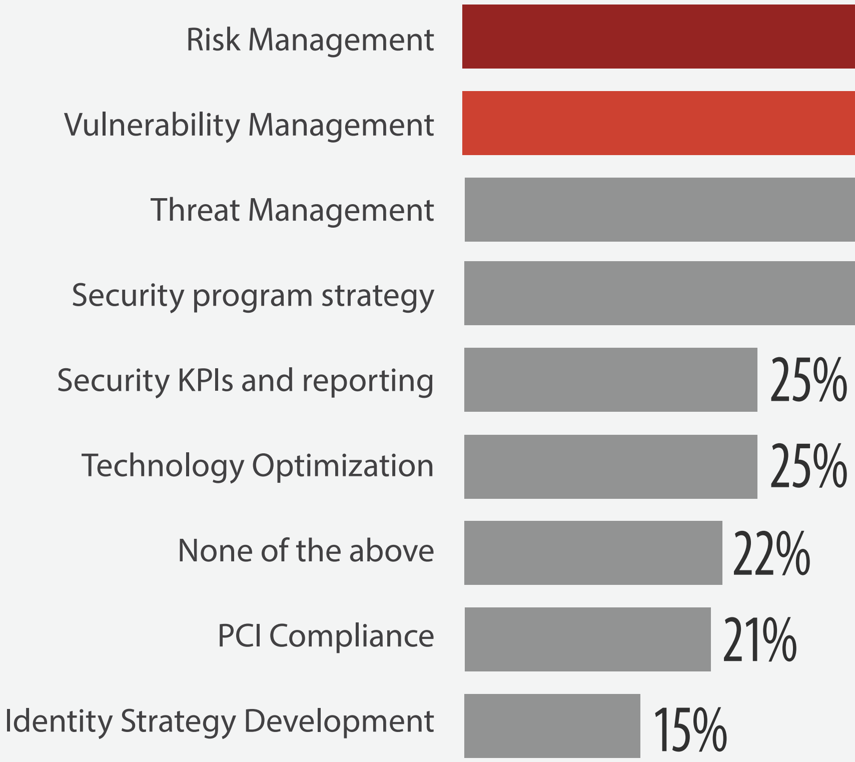
ASK YOURSELF

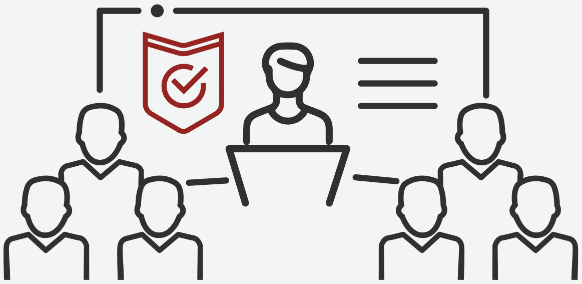
- □ What are my crown jewels? Have I identified the data and assets that are most at risk in a cyber incident?
- □ How am I currently identifying exploitable flaws in my security architecture, detective controls, and preventative controls?
- □ Is my team prepared to respond to a targeted cyber attack that leverages the latest adversarial TTPs (tactics, techniques, and procedures)?

Security Workshops

Risk and Vulnerability Management are the most popular annual workshops conducted, while Identity Strategy Development remains low on the list of priorities for many organizations.

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?





☑ ASK YOURSELF

□ Does the one-time gap assessment feedback I get reflect my business needs and help me prioritize what to tackle first?

□ Does my security roadmap reflect my enterprise maturity, risk profile and unique organizational goals?

□ Have I undergone an assessment that takes into consideration my security strategy, service needs and technology investments?

Key Threats

Of all the cyber threats facing organizations, respondents list ransomware as the top concerning threat to their business (73%). 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

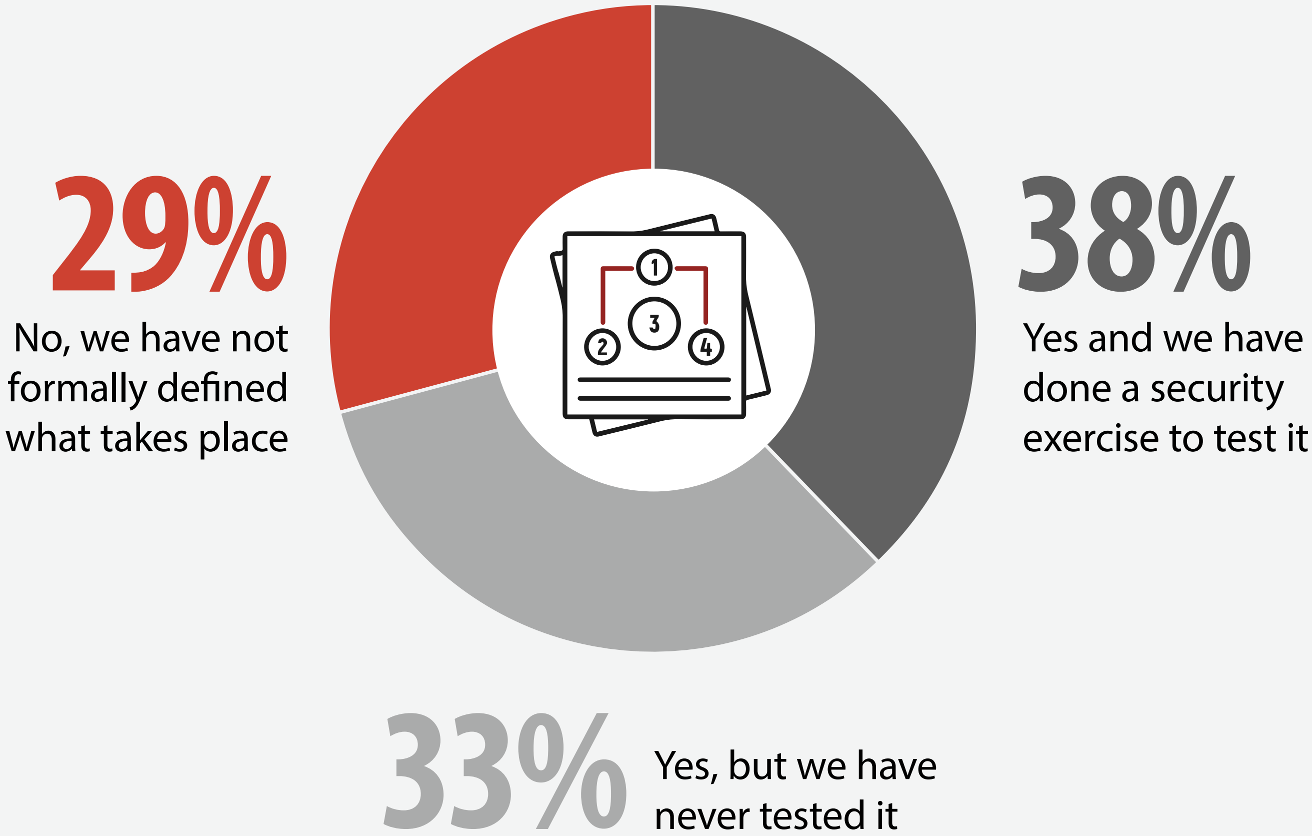
36%
Compliance findings/fines

Other 4%

Incident Response Preparedness

Only 38% of businesses have an incident response plan in place and have done a security exercise to test it.

▶ Do you have a formal incident response plan defined?



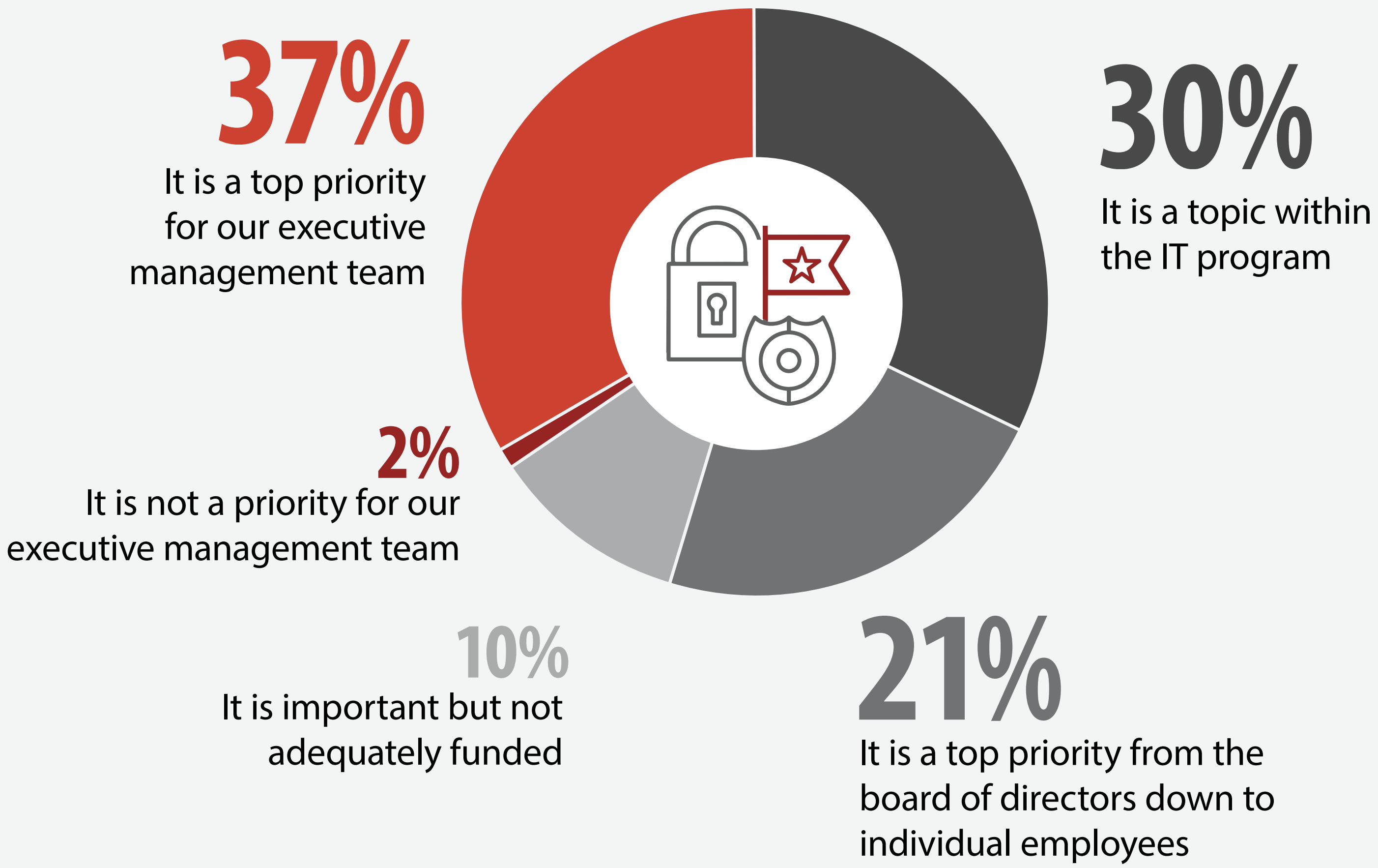
☑ ASK YOURSELF

- □ Do I have an Incident Response retainer in place with a security provider?
- □ Is my company staff, especially the executive team, aware of my security program’s readiness, plans for improvement, and capacity for response?
- □ Have I conducted regular “live-fire” incidents and simulations to test my readiness for a potential security incident?

Cybersecurity For the C-Suite

For 37% of organizations security is a top priority for their executive management team.

How important is security to your organization?



ASK YOURSELF

□ Do I know how to effectively communicate security at the executive/board level?

□ Does my organization have the proper executive metrics to measure progress and identify what risks remain to the organization?

□ Does my security plan reflect the needs and pain points of the C-level?

□ Do I have the data/findings to accurately portray the needs of the security program?

Why Use An MSSP?

The top three reasons why organizations are considering leveraging a Managed Services Provider are the lack of internal security personnel/expertise (43%), ability to respond to incidents (42%) and potential cost savings (41%).

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

43%

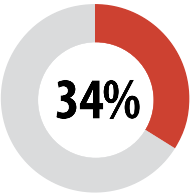
Lack of internal security personnel/expertise

42%

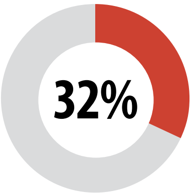
Ability to respond to incidents

41%

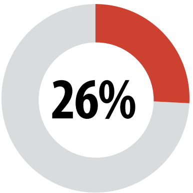
Potential cost savings



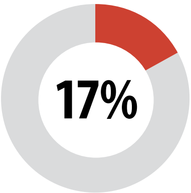
Meeting regulatory compliance mandates



Board/Executive level concern over our breach potential



A breach event at our organization



Customer/Partner demand

Deploying new cloud applications and infrastructure 10% | Mergers and acquisition activity 6% | Other 10%

Managed Security Priorities

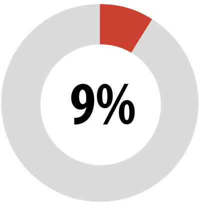
The majority of businesses list Managed Detection and Response, Managed SIEM, and Firewall Management as their top 3 priorities when it comes to Managed Security Services.

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

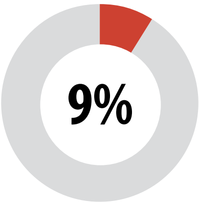
26%
Managed detection and response

25%
Managed SIEM

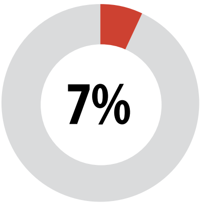
14%
Firewall management



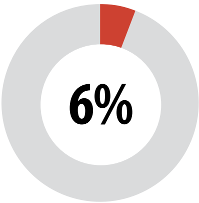
Endpoint management



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

According to responses, 24/7 coverage, cost, and the ability to integrate existing security technology are the top 3 factors when selecting a provider.

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

63%

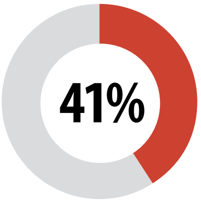
24/7 coverage of security operations

54%

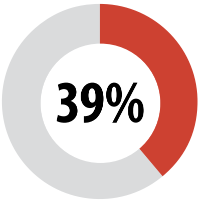
Solution cost

50%

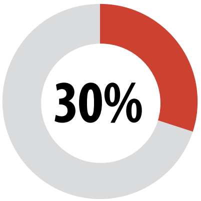
Ability to integrate/ leverage our security technology stack



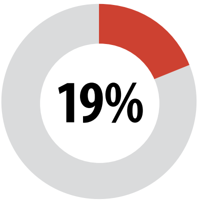
Supported systems or technologies



Reputation of company and leadership



Ability to customize reporting



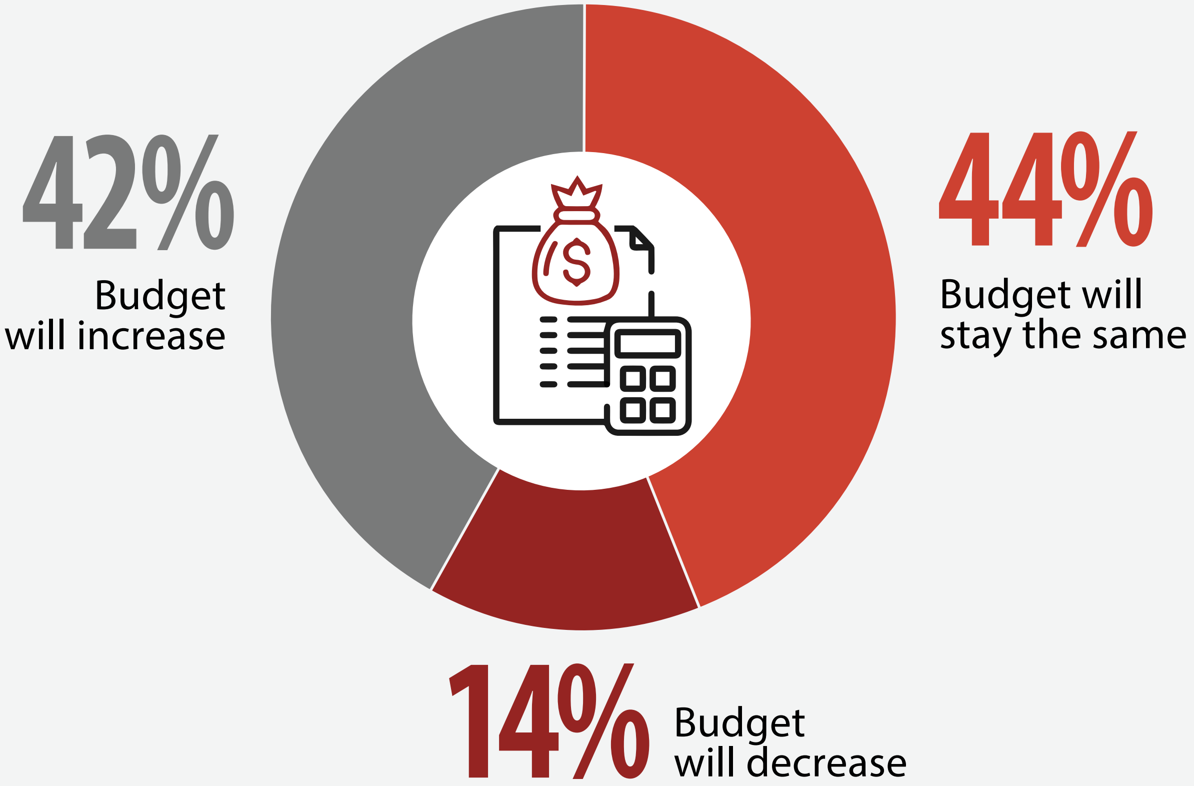
Location/Proximity (Ability to interact with a local or regional analyst)

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 will increase. Only 14% expect a decline.

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



ASK YOURSELF

□ Is my budget based on tools and technology, or rather a shared understanding of risks to our business and how to mitigate them?

□ Is our budget aligned with a security roadmap for the next 12-24 months?

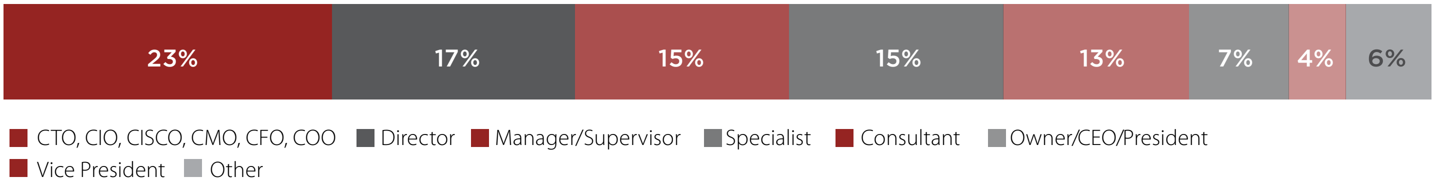
□ Do we have a thorough understanding of our current tool stack licensing, renewal and support details?

□ If my budget will remain the same, what are we doing to mitigate vulnerabilities and a growing threat landscape?

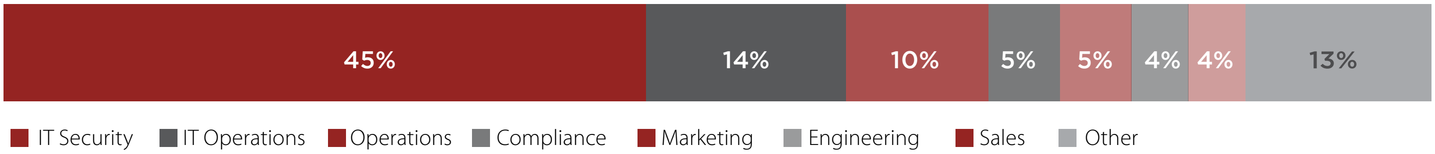
Methodology & Demographics

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 a spectrum of company sizes and industries, representing a balanced cross-section of organizations.

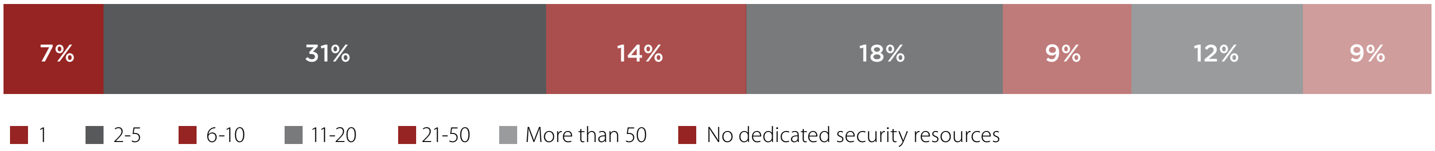
CAREER LEVEL



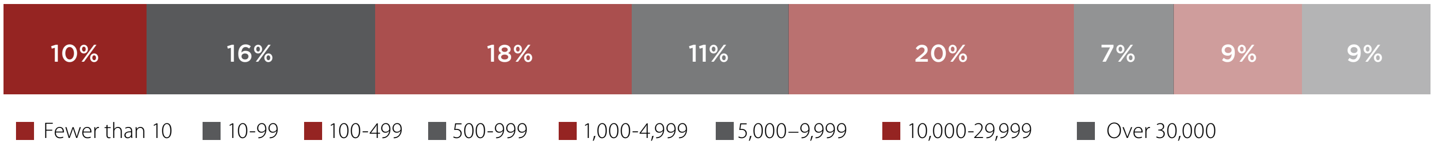
DEPARTMENT



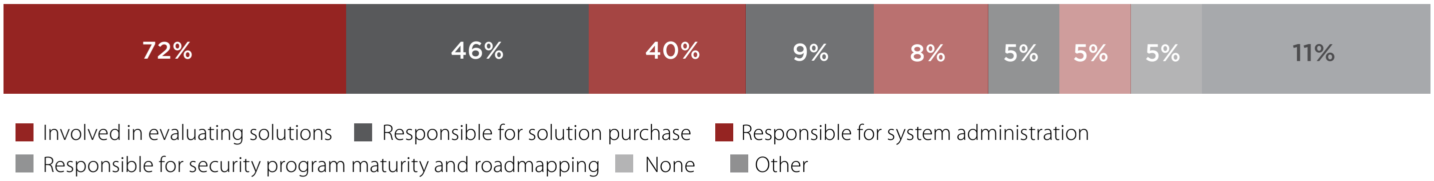
IT SECURITY TEAM HEADCOUNT



COMPANY SIZE



LEVEL OF INVOLVEMENT IN SECURITY



HERJAVEC GROUP

Herjavec Group has been ranked as the world's most innovative cybersecurity company by Cybersecurity Ventures and a top global Managed Security Services Provider by MSSP Alert. We offer products and services to keep enterprise organizations secure while we help solve the industry's greatest challenge – a severe cybersecurity labor shortage. With 5 global Security Operations Centers, emerging technology partners and a dedicated team of security specialists, Herjavec Group is well positioned to be your organization's trusted advisor in cybersecurity.

Herjavec Group understands that technology alone cannot prevent today's cyber attacks. We have expertise in comprehensive security services, including **Managed Security Services** (SOC Operations, Threat Detection, Security Technology Engineering) & **Professional Services** (Advisory Services, Identity Services, Technology Architecture & Implementation, Threat Management, and Incident Response).

MANAGED SECURITY SERVICES

- SOC Operations
- 24/7 Threat Detection
- Security Technology Engineering
- Managed Detection & Response
- Managed Phishing

PROFESSIONAL SERVICES

- Advisory Services
- Identity Services
- Technology Architecture & Implementation
- Threat Management
- Incident Response

Recognized Industry-Wide

BEST IAM SERVICE

SECURITY SERVICES LEADER

IDC *Analyze the Future*

LEADER IN MANAGED SECURITY SERVICES

SECURITY COMPANY OF THE YEAR

CDM CYBER DEFENSE MAGAZINE

#1 ON THE CYBER SECURITY 500

TOP 5 ON THE TOP 200 MSSPs

Accelerate Your Cybersecurity Journey

✓ **COMPREHENSIVE SECURITY EXPERTISE**
We offer Advisory, Implementation, Identity, Managed Security & Incident Response Services.

✓ **100% CYBERSECURITY FOCUSED**
We are laser-focused on security & recognized as one of the world's most innovative cybersecurity players.

✓ **UNBIASED, VENDOR AGNOSTIC APPROACH**
We partner with best of breed technology providers and are on the pulse of emerging technology trends, to design and protect your security stack.

✓ **SPEED & AGILITY IN MULTI-TECH ENVIRONMENTS**
Our cyber experts support the world's largest banks, gaming companies and utility providers - offering customized and flexible solutions.

✓ **GLOBAL APPROACH WITH CROSS CLIENT LEARNINGS**
We have expert knowledge of regional and industry directives. Threat intelligence and data enrichment across industry & region benefit our global clients.