WHITE PAPER

nuspire

First Annual CISO Research on Challenges and Buying Trends: A Focus on Prevention

200 CISOs and ITDMs Provide Insights into Security Concerns and Outsourcing Priorities

nuspire.com

Introduction

Peer perspectives on cybersecurity give you an opportunity to evaluate your organization's current state and initiate discussions about your strategy, staff and budget. To collect data, Nuspire recently conducted its first annual survey* with 200 chief information security officers (CISOs) and IT decision-makers (ITDMs). We explored pain points, priorities, the purchase process and product/service awareness.

Only 4% of CISOs and ITDMs manage all of their cybersecurity needs in-house, so outsourcing clearly is a big part of cybersecurity plans and programs. But CISOs say budgets are somewhat constrained by senior leaders who aren't invested enough in the issues. As a result, they're willing to spend money to outsource only certain aspects of cybersecurity.

Given the challenges and concerns of CISOs and ITDMs, their views on outsourcing priorities are mostly sensible but surprising in a few areas. This paper presents highlights of the research. Read on to discover what's top of mind for CISOs and ITDMs:

- Use the findings as a touchstone for your security decisions.
- Discover which security services are perceived as must-haves.
- Explore CISO buying trends.

What Makes This Research Compelling? Duo™ MaxDiff

We gathered information using two methodologies: (1) traditional survey questions that ask respondents to choose one answer or all that apply, and (2) the Duo™ MaxDiff approach that asks respondents to make a choice based on two dimensions of interest instead of one. In this analysis, the dimensions are "most concerning issues" and "most likely to outsource to a cybersecurity provider." Duo™ MaxDiff increases survey accuracy, enables the greater differentiation that leads to actionable results, and helps identify the order and magnitude of results across a quadrant of dimensions.

Key Survey Findings

66% of respondents feel their companies are somewhat vulnerable or extremely vulnerable to attacks on your company's data.

Within digital environments, 42% say cloud applications are the most susceptible to attack, followed by 40% who say end users.

56% and 58% of senior leaders, respectively, are involved and knowledgeable, but limited understanding and a reactive mindset constrain budgets.

70% are likely to outsource to support overall security program improvements and obtain 24/7/365 protection.

nuspire

CISOs and ITDMs generally feel confident about their cybersecurity programs and strategy, but challenges persist. Certain themes underlie four key pain points: the transition to remote work, the rate of change in the threat landscape and endpoint security.

1. Strengthening protection against cyberattacks using technology advancements and automation to lower risk, increase device security and prevent breaches.

Two-thirds of respondents believe their companies are somewhat vulnerable or extremely vulnerable to attack. Within digital environments, cloud applications are identified by 42% as the most susceptible to attack, followed by end users, cloud infrastructure and endpoints. In addition, 31% say the lack of visibility into the most vulnerable assets due to budget constraints is another cause of system vulnerabilities.

Cloud, remote end users and remote endpoints are newer aspects of the threat landscape. The pandemic caused IT/security teams to shift resources from traditional perimeter-based projects to rapid deployments that protected home-based workers. Then, as the pendulum swung back to settle on hybrid workforces, IT/security teams had to adjust again.

"The biggest challenge I currently face at my organization concerning cybersecurity is data breach due to remote work."

"The biggest challenge is finding the right… technology/mechanism to prevent attacks before they occur rather than take action once the attack has occurred."

"…a talent gap, a lack of guidance from professionals… [leads to the need for constant trial and error]."

2. Attracting and retaining highly skilled and better trained cybersecurity professionals.

Two-thirds of respondents strongly agree or somewhat agree that talent is difficult to hire – a trend that has disrupted the industry for many years and is likely to continue. Talent shortages can create security vulnerabilities that can linger for weeks or months, increasing risk. Many threats aren't detected until an incident occurs.

- More than 55% of respondents worry that their cybersecurity teams are so busy they might not detect an attack until it's too late.
- 34% say that upgrading and enhancing cybersecurity skills would have the biggest impact on their security program.
- Nearly 25% of respondents say the biggest impact on their security programs is threat intelligence and up-to-the-minute actionable information about new threats – but this is an area that requires trained professionals to deliver real-time and on-demand threat hunting.

To alleviate skills shortage, many organizations rely on outsourcing. Given the number of "want to do" and "need to do" security choices, however, CISOs and ITDMs juggle concerns with budget availability.

nuspire

3. Educating end-user employees to avoid attacks.

Employees can be your front line of defense when they're security aware. Without regular security awareness training, employees can unknowingly let attackers in. Cloud migration expands the attack surface, so training needs to go beyond the employees who work directly with sensitive data or financial information. For example, train developers who are writing application code and people who buy and configure cloud services.

CISOs worry about end-user vulnerabilities related to ransomware, phishing and data breaches. All are well-known and well-publicized threats, so no surprise that one survey respondent calls out the risk of stolen customer information and a potential "public relations nightmare." Half of respondents cite human error and lack of internal employee training as the No. 1 reason for IT system vulnerabilities. And the high-risk departments? IT, finance and sales/marketing. These departments are targeted by threat actors hoping to gain access to IT servers and sensitive customer/vendor data and email accounts.

"More employees in my organization need to be trained in threat detection. As we have remote workers, much of the cybersecurity falls on individuals, and they need to learn how to recognize threats and avoid them."

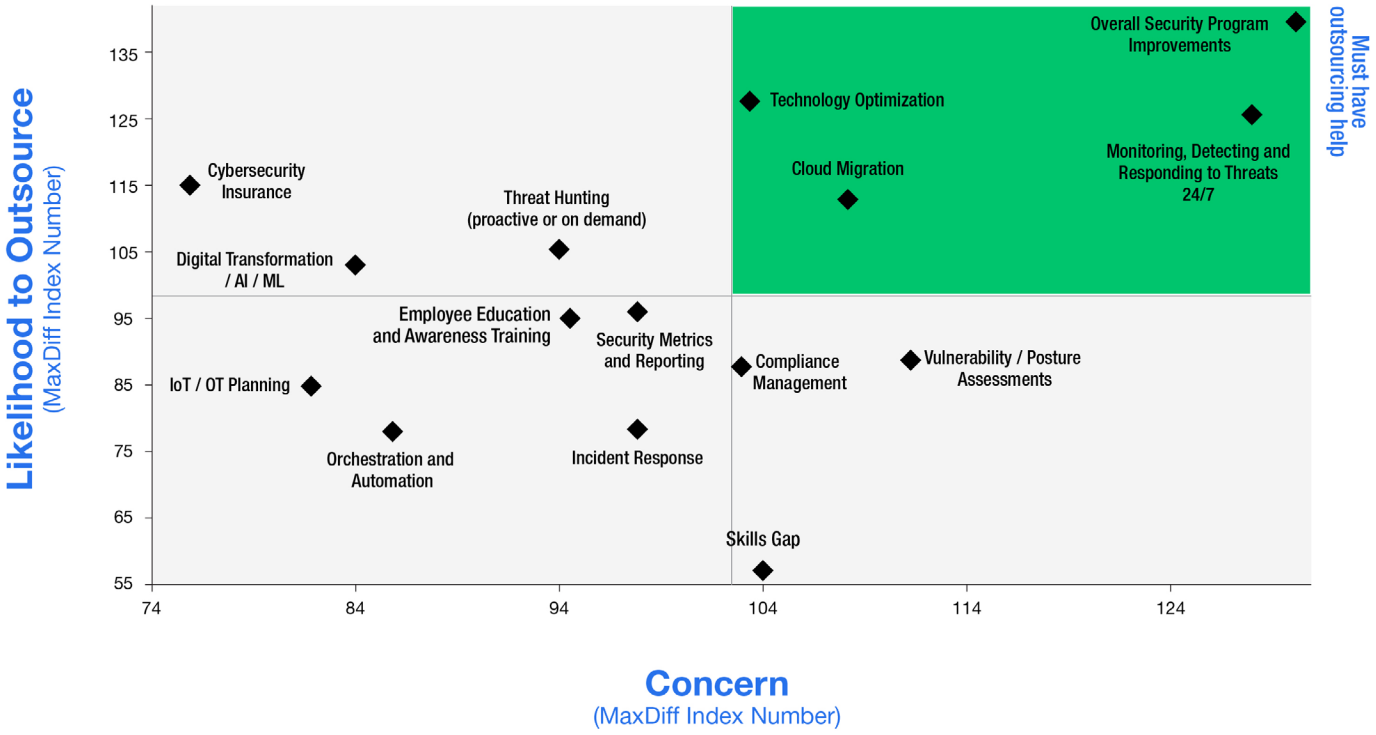
4. Improving reliable protection for remote workers.

Remote work amplifies concerns about employee education. Survey respondents report that remote work introduces "…more ways for hackers to attack our systems…" and "with remote work, our cybersecurity teams are unable to properly secure all of the devices used to access our systems."

What's most susceptible to cyberattacks in digital environments? Approximately one-third of respondents say email and collaboration tools, and 26% cite supply chain and third-party risk.

Figure 1 ranks the cybersecurity services that CISOs and ITDMs are most likely to outsource based on the Duo MaxDiff approach, which forces respondents to make a choice based on the two dimensions described on page 2. When asked about what's most important to accomplish their business objectives, respondents name many services that directly or indirectly protect remote workers.

Figure 1. High priority: staying up to date and optimizing existing technology



CISOs and ITDMs address challenges through outsourcing services that point to the importance of prevention. The research identifies four security program must-haves – services for which CISOs and ITDMs are willing to spend money.

Overall security program improvements.

Respondents point to improvements such as staying current with threats and updates based on industry and threat intelligence. At the top of the list (see Figure 1) are cloud security posture management (CSPM) and cloud access security broker (CASB), which are cited by 43%. Following closely is endpoint detection and response (EDR).

Monitoring, detecting and responding to threats 24/7.

EDR and MDR are core technologies to add to or enhance technology stacks. Obtaining EDR and MDR from a service provider addresses staffing/skills shortages and provides up-to-date technology.

Technology optimization and integrations to ensure best use of existing technology.

Few decision-makers opt for rip-and-replace solutions given budget constraints. The right managed security services provider (MSSP) can help you take stock of current assets, explore risk tolerance and make every dollar count.

Cloud migration and protection of the expanded attack surface.

An integrated cybersecurity strategy increases protection for

The Top Three Types of Services Most Likely to be Outsourced

1. **Overall security program enhancements, specifically staying current with threats** and updates based on industry and threat intelligence
2. **24/7 threat monitoring, detection and response**
3. **Technology optimization and integrations** to ensure best use of existing technology

nuspire

Figure 2. Top 10 outsourced services

Support for program improvements, 24/7 protection and tech optimization are biggest focus areas

	Duo Max Diff: Most Likely To Outsource To A Cybersecurity Provider	Total N=200
1	Overall security program improvements - Staying current with threats and updates based on industry and threat intelligence	140
2	Monitoring, detecting and responding to threats 24/7	127
3	Technology optimization and integrations to ensure best use of existing technology	127
4	Cybersecurity insurance	115
5	Cloud migration	112
6	Threat hunting (proactive or on demand)	105
7	Digital transformation / AI / ML	102
8	Security metrics and reporting	96
9	Employee education and awareness training	94
10	Vulnerability / posture assessments	89
11	Compliance management	89
12	IoT / OT planning	86
13	Orchestration and automation	81
14	Incident response	80
15	Skills gap	56

Top	>120	115-120	110-115	100-110	90-100	70-90	<70

remote workers and sends the right message to senior leaders.

Additionally, Figure 2 identifies other priorities that CISOs and ITDMs are willing to outsource but less so than the must-haves. These are:

Threat hunting (proactive or on demand). 24/7/365 threat hunting is vital to maintaining a strong security posture, but it's time-consuming. In-house staffs can do only so much.

Cybersecurity insurance, a complex, fast-changing and important element of security programs. It's likely ranked below must-have level because this topic requires a substantial learning curve.

The least likely candidates for outsourcing include:

Vulnerability/security posture assessments – a missed opportunity because assessment findings are highly effective in showing decision-makers how to allocate resources efficiently to address gaps or concerns.

Incident response, which can make or break an organization that experiences an intrusion or breach. Possibly CISOs and ITDMs believe their in-house incident response is adequate, or they view incident response as a service they can get when they need it, or they have cyber insurance that coordinates incident response.

Employee education – although this topic fell into the "most important/concerning" category, organizations are not as likely to outsource education compared to services such as MDR and threat hunting. It appears that CISOs and ITDMs believe they can provide the necessary security awareness training internally.

Buying Trends Suggest Prevention Is Paramount

While CISOs and ITDMs cite many security concerns, they appear to have a fairly high level of confidence in their current cybersecurity programs and overall strategy. Top concerns are focused on improvements to help prevent attacks. Due to limited budgets, however, CISOs and ITDMs cannot outsource some of the tasks they're willing to outsource. As a result, organizations may choose to outsource more commoditized services and keep nuanced and unique aspects of the security program in-house.

Learn more about the research by **viewing a webinar** in which two industry veterans discuss the findings, including the top 10 concerns and the top 10 most likely to be outsourced services. Peer perspectives may be just the door-opener you need to revisit security and budget decisions.

**Unless otherwise noted, stats and findings come from Nuspire research (n=200, CISOs and ITDMs in the U.S. who represent 14 industries and companies ranging from 500 to 10,000+ employees) conducted in Q2 2022.*

A Duo™ MaxDiff approach was used to analyze the data.

(866) 526-8333

support@nuspire.com

nuspire.com

nuspire

Nuspire is a leading managed security services provider (MSSP) that is revolutionizing the cybersecurity experience by taking an optimistic and people first approach. Our deep bench of cybersecurity experts, world-class threat intelligence and 24x7 security operations centers (SOCs) detect, respond and remediate advanced cyber threats. We offer comprehensive services that combine award-winning threat detection with superior response capabilities to provide end-to-end protection across the gateway, network and endpoint ecosystem. Our client base spans thousands of enterprises of all sizes, across multiple industries, and achieves the greatest risk reduction per cyber-dollar spent. At Nuspire, we are laser focused on delivering an extraordinary cybersecurity experience that exceeds client expectations.

For more information, visit nuspire.com and follow @Nuspire

nuspire.com
LinkedIn @Nuspire
Twitter @NuspireNetworks