Nuspire Annual Study:

Top 10 CISO Buying Trends of 2022

August 31, 2022

Study Background & Methodology

Why We Did It

- ✓ Explore key trends and understand what drives decision making
- ✓ Conduct a benchmark study that serves as a foundation for annual changes over time
- ✓ Help inform our services that our typical clients deem most important

Key objectives:

- ✓ Identify CISOs' key drivers of where CISOs spend their time and where they seek outsourcing help
- ✓ Understand motivations and priorities of their outsourced cybersecurity spend
- ✓ Determine how key drivers or CISO concerns correlate with whether an organization uses their own staff/resources or whether they outsource

Methodology

Benchmark Quantitative Survey

Online survey

Duo MaxDiff

Audience:

IT Security Decision Makers in the U.S.

N=200 interviews of CISOs and IT security decision makers across verticals

500-10K employees

Budgets $100K – $3M+ cybersecurity spend

Key Findings

1 While decision makers are generally confident in their organization's cybersecurity measures, a majority feel their company is susceptible to attack

» While nearly 7 in 10 (69%) say their company's investment in cybersecurity exceeds other companies, two-thirds (66%) say they are vulnerable to attack

2 End-users are a significant concern point for decision makers. More education is needed to prevent ransomware and phishing attacks – especially in an era of remote work

» Half (50%) say human error/lack of internal employee training is the primary reason for IT vulnerabilities

3 While senior leaders are generally knowledgeable, many decision makers feel they are not invested enough in the issues to provide the budget required

» 9 in 10 say their senior leaders are involved (92%) and knowledgeable (92%) about their organization's cybersecurity measures - At the same time, many feel they are not invested enough to increase their cybersecurity budgets

4 Decision makers are most likely to outsource services related to overall security program improvements and protecting their organization around the clock

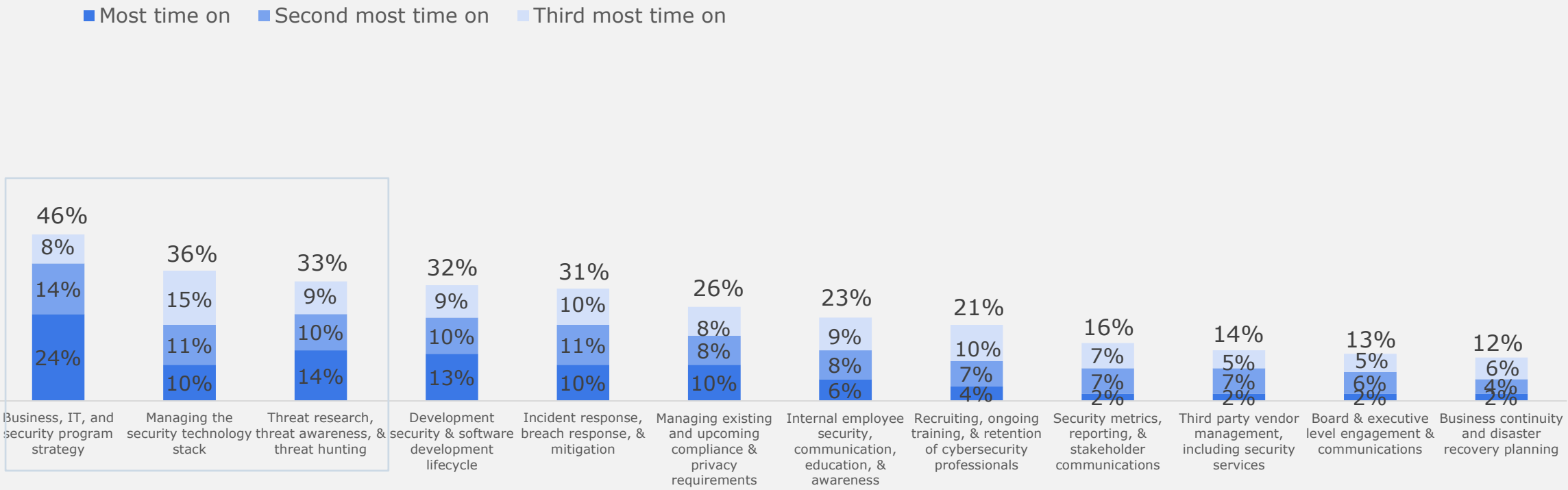
» The top 2 items that are most concerning and most likely for decision makers to outsource are "Overall security program improvements - Staying current with threats and updates based on industry and threat intelligence" and "Monitoring, detecting and responding to threats 24/7"

Detailed Findings

Nearly 1/4 of decision-makers

Spend the most time on business, IT and security program strategy – trying to stay up to date and managing tech stack.

Time Spent
Showing %, ranked by "total time spent"

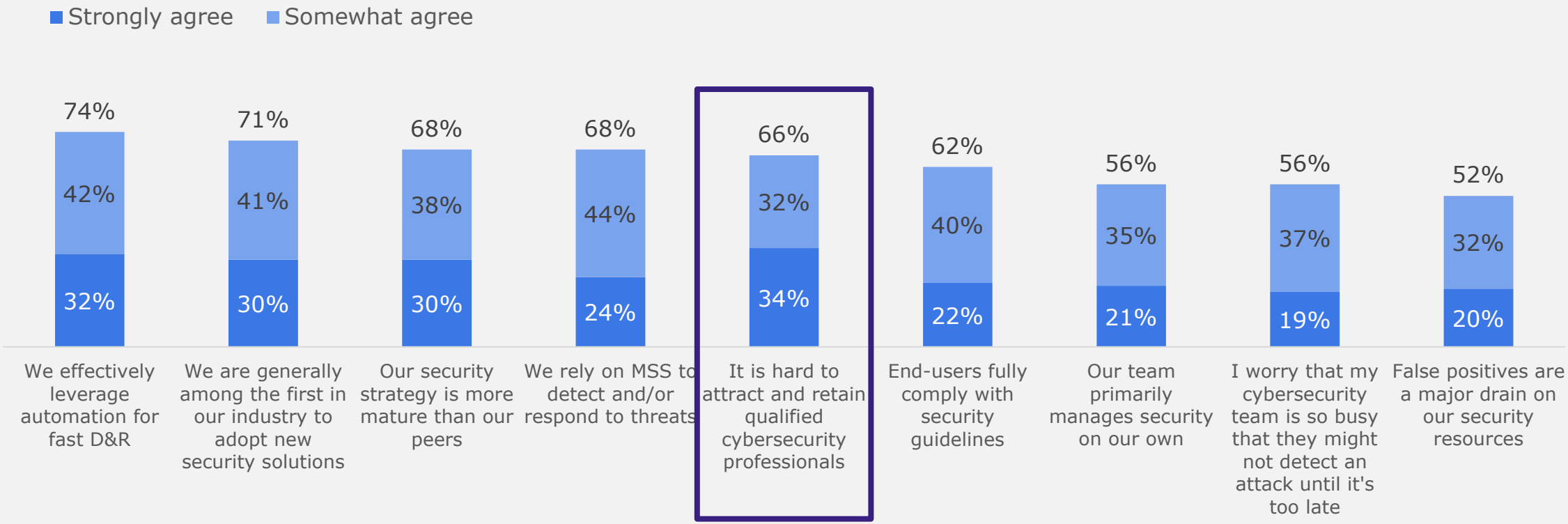


qTIME_SPENT. Thinking about your day-to-day responsibilities, which of the following do you spend the most time on? Please rank up to 3.

Most are confident in their current cybersecurity programs and overall strategy

However, they find it most difficult to attract and retain qualified cybersecurity professionals

Agree or Disagree with Statements
Showing %, ranked by "total agree"



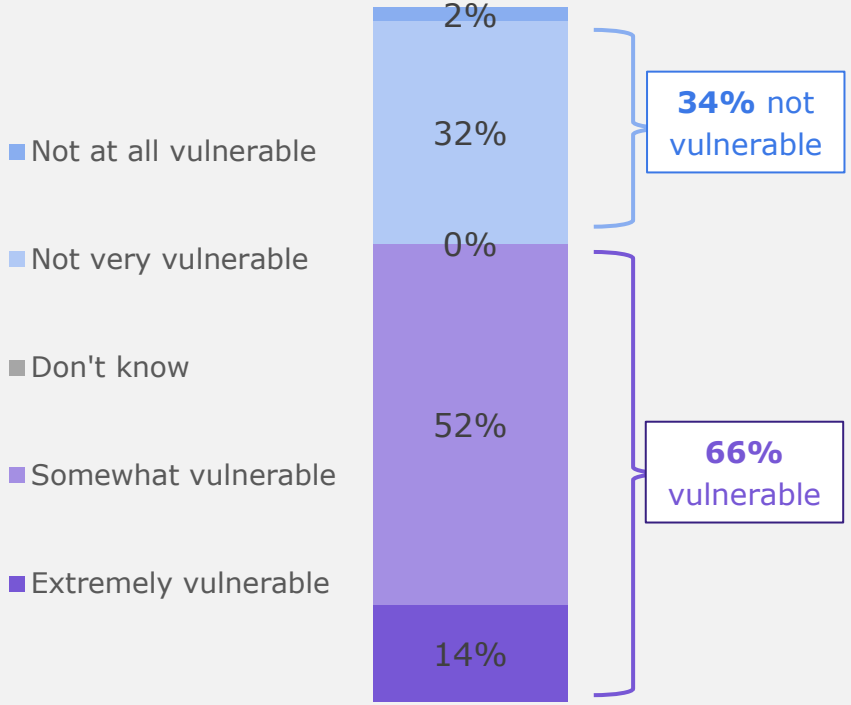
gSTATEMENT1-9. How much do you agree or disagree with the following statements regarding your organization?

Despite confidence in their program, 2/3 believe organization is still vulnerable to attack

Cloud applications, end users and cloud infrastructure highlighted as the most susceptible to attacks

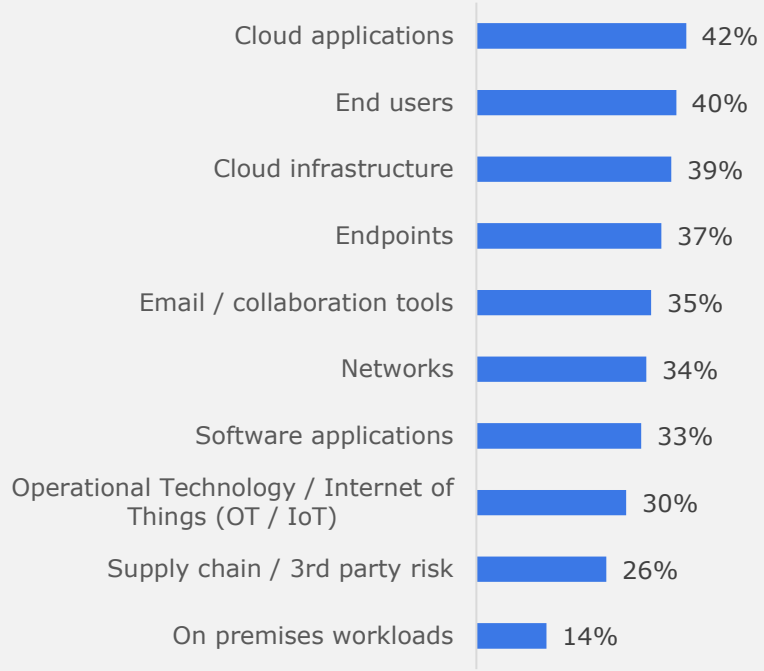
Vulnerability of Organization to Cyberattacks

Showing %



Aspects of the Digital Environment Most Susceptible to Cyberattacks

Showing % ranked



qVULNERABLE. How vulnerable do you believe your organization is to a significant cyberattack (e.g., one that disrupts business processes, causes brand reputation damage, or leads to theft of sensitive data)?
qSUSCEPTIBLE. What aspects of your digital environment do you think are most susceptible to attacks? *Please select all that apply.*

The biggest challenge: transition to remote work

Amplifies need for employees to be more aware of how to protect themselves – and the company – from potential cyberattacks

Biggest Cybersecurity Challenge
Showing Open-Ended Responses

REMOTE WORK	*"The biggest challenge I currently face at my organization concerning cybersecurity* ***is data breach due to remote work****."*	*"There are more ways for hackers to attack our systems today.* ***With remote work, our cybersecurity teams are unable to properly secure all of the devices*** *used to access our systems."*
RATE OF CHANGE	*"The biggest challenge I face is the* ***ever-adapting nature of cyberattacks*** *and malicious threats that evolve with security upgrades."*	*"No matter how many [security measures] we put up it just* ***never seems to be enough--we are constantly having to build new programs to put up more****."*
ENDPOINT SECURITY	*"The biggest challenge we face is* ***employees not fully understanding their role*** *in preventing security issues, especially in a work from home environment."*	*"Employees not understanding what can cause security issues and/or breaches. They're* ***not educated well enough about the risks****."*

qCHALLENGE_OE. Thinking of cybersecurity at your organization, what would you say is the single biggest challenge you currently face in your role?

End-user vulnerabilities particularly concerning when it comes to ransomware and phishing attacks

IT, finance and sales/marketing departments viewed most vulnerable

Most Worrisome Threat
Showing Open-Ended Responses

Ransomware

*"Ransomware on **employee-owned endpoint devices.**"*

Phishing

*"The **most common** cybersecurity threat employees fall for is phishing attacks."*

Data Breaches

*"**Customer information being stolen** and the PR nightmare that would have caused."*

Most Vulnerable Department
Showing Open-Ended Responses

IT

*"The department that worries me the most is the IT department for the simple fact of **having access to the servers.**"*

Finance

*"Most worried about the finance department, **the department has a lot of money.**"*

Sales/Marketing

*"Our sales & marketing teams are **dealing with a number of outside clients, vendors and general e-mail accounts**."*

qBREACHWORRY_OE. In the last year, which type of security threat did you most worry about?
qVULNDEPT_OE. Which department do you worry is most vulnerable to a cybersecurity breach?

Half view a lack of internal employee training as their top driver of system vulnerabilities

Main Reasons for IT System Vulnerabilities
Showing % ranked

Types of Vulnerabilities	
Human error / lack of internal employee training	**50%**
External threat actors / nation states	36%
Legacy systems and non-integrated technology	36%
Rate of technological change is too fast to keep up with	36%
Lack of visibility into most vulnerable assets due to budget constraints	31%
Inability to appropriately prioritize vulnerabilities	30%
Appropriate risk / vulnerability assessment	28%
Lack of budget	26%
Insider threats	24%
Shadow IT	20%
None of the above	2%

qVULNERABILITY_REASONS. What, in your view, are the main reasons for vulnerabilities in IT systems today? Please select all that apply.

Decision makers most likely to outsource CSPM, CASB and EDR to manage vulnerabilities

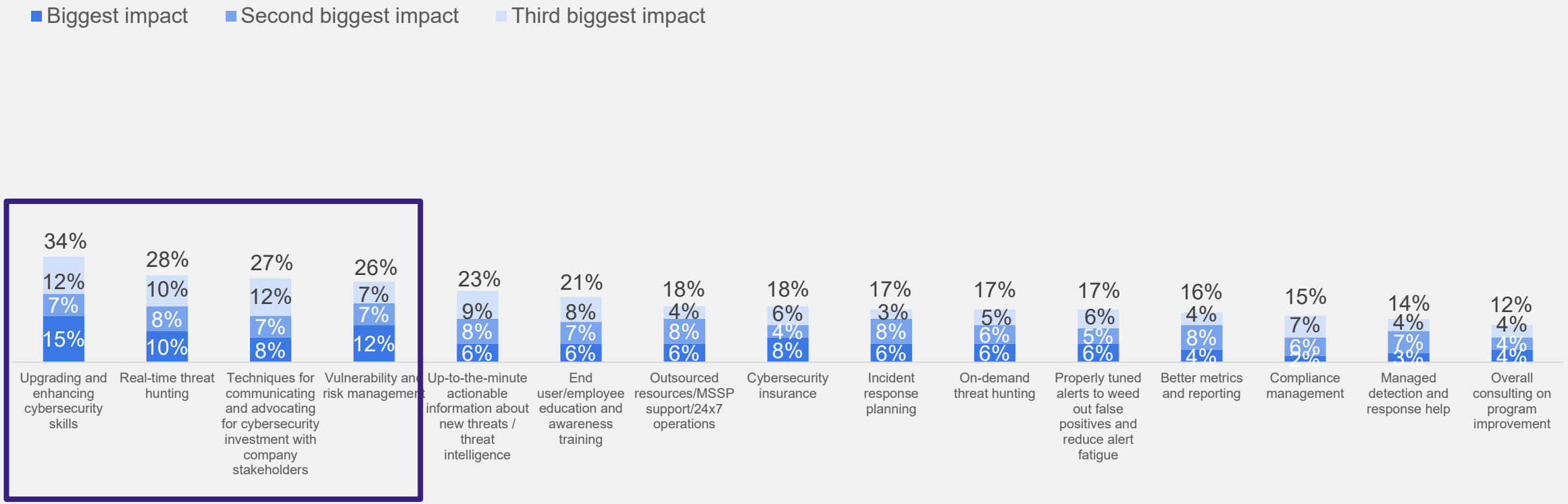
Very few manage all their cybersecurity needs fully in-house

Cybersecurity Services Outsourced	
Cloud Security Posture Management (CSPM)	**43%**
Cloud Access Security Broker (CASB)	**43%**
Endpoint Detection and Response (EDR)	**40%**
Secure WiFi	36%
Managed Firewall	36%
Managed Security Services (MSS)	34%
Security Information and Event Management (SIEM)	32%
Software-Designed Wide Area Network (SD-WAN)	32%
Secure Access Service Edge (SASE)	32%
Managed Detection and Response (MDR)	28%
Extended Detection and Response (XDR)	24%
None of the above / Our organization does all of our cybersecurity in-house	4%
Other	0%

qDETECTION_RESPONSE_TYPE. What type(s) of cybersecurity services does your organization currently outsource? *Please select all that apply.*

Upgrades/enhancements to things like threat hunting and risk management would have the biggest impact

Impact on Security Program
Showing %, Ranked by "total impact"



gIMPACT1-3. Over the next year, which of the following would have the biggest impact on your organization's security program? Please rank the top 3 most impactful resources.

When asked about biggest impact to security program…

Respondents consistent in citing solutions that help fend off cyberattacks – technology stack, skilled professionals and end-user education

Missing Technology, Skill or Service
Showing Open-Ended Responses

1) General technology advancements/automation to better prevent against cyberattacks
2) Highly skilled and better trained cybersecurity professionals
3) More end-user employee education around avoiding attacks
4) More reliable protection for remote workers

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

*"[There is a] **talent gap**, a lack of guidance from professionals, [leading to] the need for constant trial and error."*

*"**Increase in advanced technology** with regards to firewalls and cyber security **to help prevent hacks and down time**."*

*"**Better control of people working remote** due to covid to ensure their devices are being secure and cannot be breached."*

*"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**."*

qRESOURCE_OE. What is the one missing technology, skill or service that would have the biggest impact to your organization's cybersecurity?

Concerns and Needs for Outsourcing Help

Duo MaxDiff

Used to identify key pain points and priorities for Decision Makers

Maximizes insights by asking respondents to make a choice based on two dimensions of interest instead of one, in this case ***most likely to outsource to a cybersecurity provider*** *and* ***most concerning****.*

A Duo MaxDiff allows us to:

- ✓ **Increase accuracy** by eliminating response biases and other systematic errors
- ✓ **Provide more actionable results**. Items are shown in direct competition, which allows us to tease out the differences between items
- ✓ Produce individual "utilities" on each dimension of interest, allowing us **to better identify both order and magnitude of the results across a quadrant of dimensions**

Top 10 concerns

Security program improvements, MDR and vulnerability/posture assessment most important

	Duo Max Diff: Most Concerning	Total N=200
1	Overall security program improvements - Staying current with threats and updates based on industry and threat intelligence	132
2	Monitoring, detecting and responding to threats 24/7	129
3	Vulnerability / posture assessments	110
4	Cloud migration	108
5	Technology optimization and integrations to ensure best use of existing technology	105
6	Skills gap	104
7	Compliance management	102
8	Security metrics and reporting	97
9	Incident response	97
10	Employee education and awareness training	95
11	Threat hunting (proactive or on demand)	94
12	Orchestration and automation	85
13	Digital transformation / AI / ML	84
14	IoT/OT planning	83
15	Cybersecurity insurance	75

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

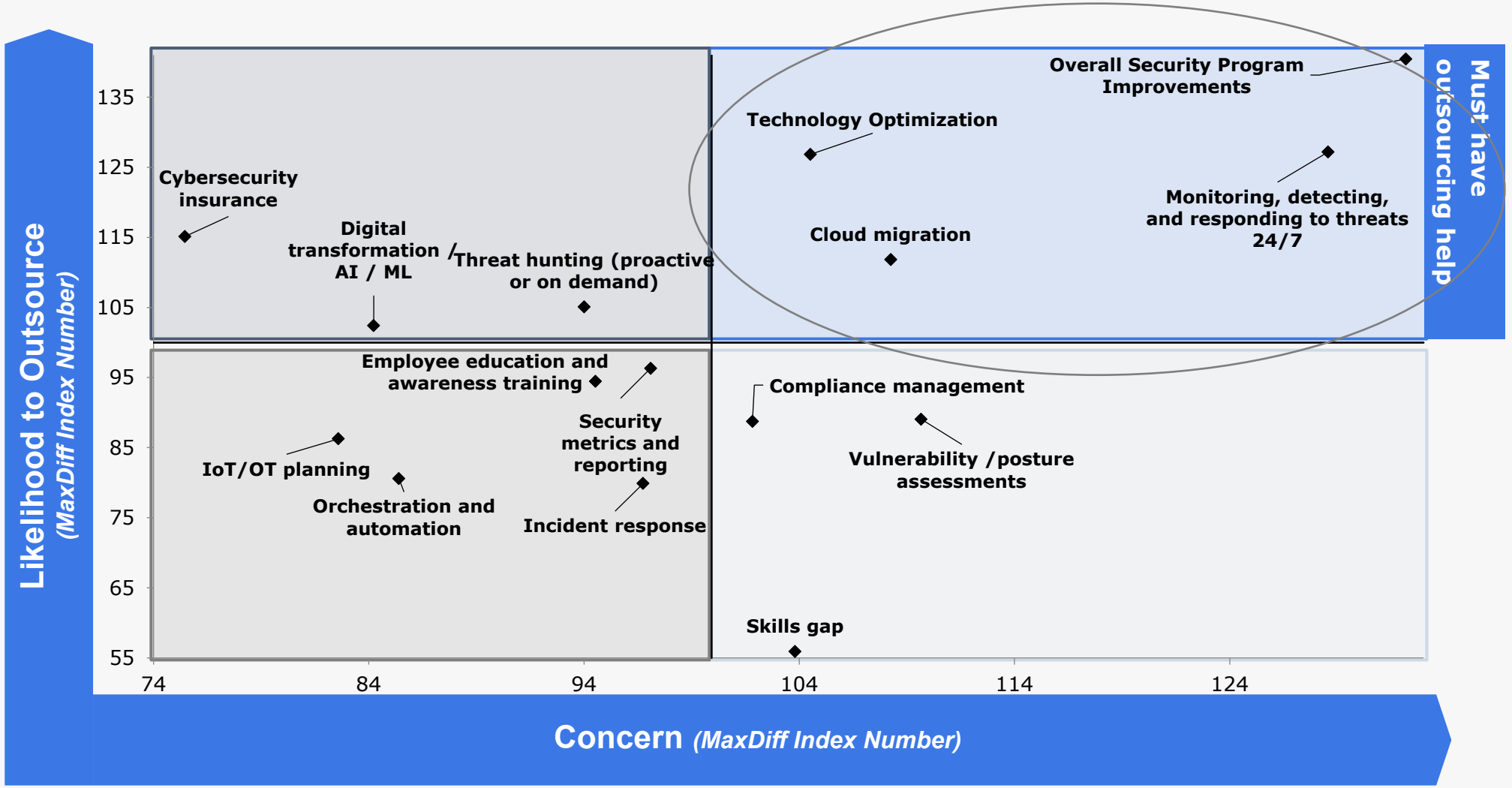
Top 10 outsourced services

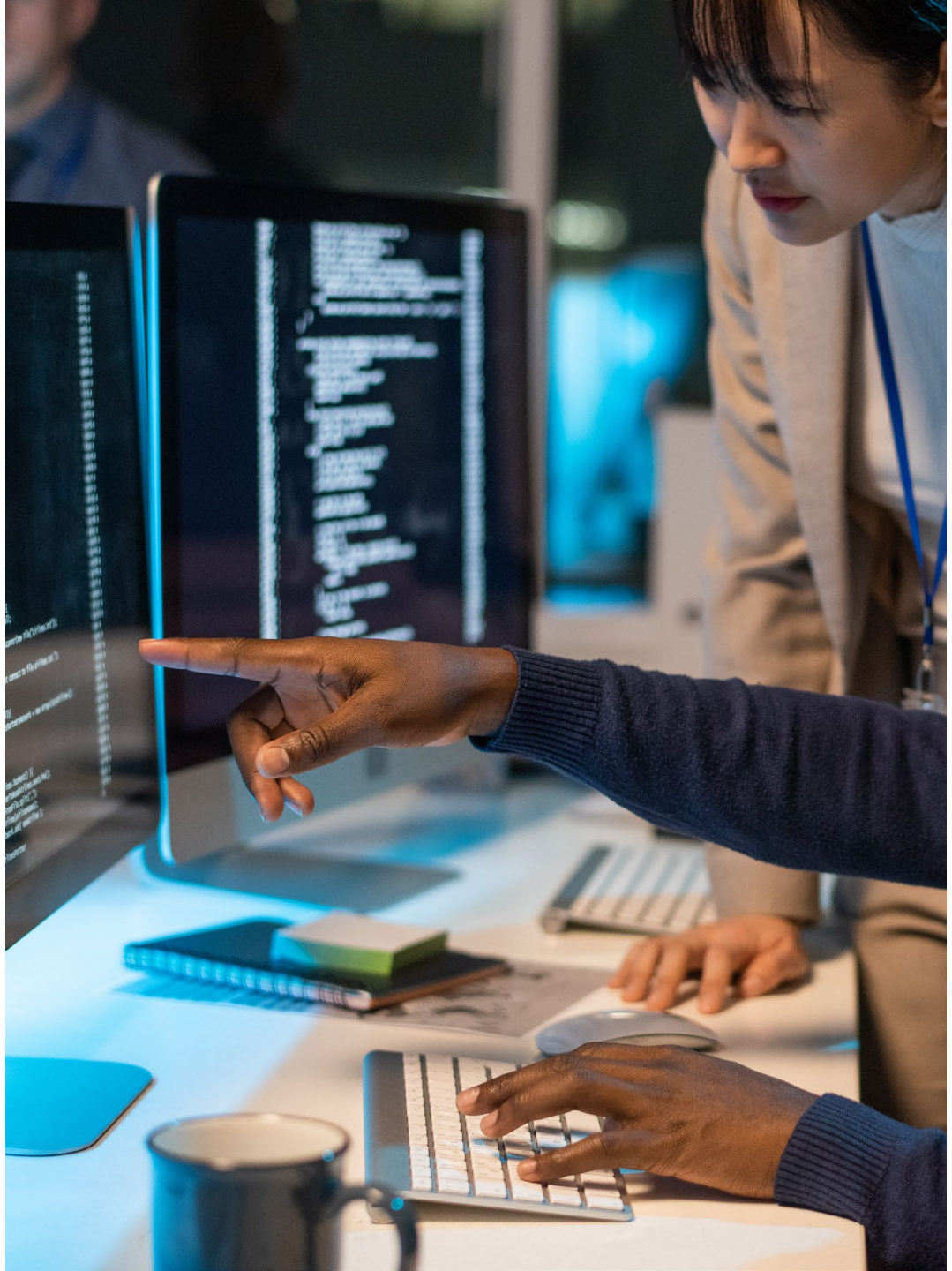
Support for program improvements, 24/7 protection and tech optimization are biggest focus areas

	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

High priority: staying up to date and optimizing existing technology





Next Webinar

Top 5 Drivers of Managed Detection and Response Adoption, Featuring IDC

Thursday, Sept. 22 | 12 p.m. ET

Presenters

Craig Robinson, Program Director, Security Services, **IDC**

Michelle Bank, Chief Product and Marketing Officer, **Nuspire**

Jonathan Nguyen-Duy, Vice President, Global Field CISO, **Fortinet**

nuspire | FORTINET

IDC

Thank you.

Contact Us

webinars@nuspire.com
nuspire.com

Michelle Bank
michelle.bank@nuspire.com

J.R. Cunningham
jr.cunningham@nuspire.com

August