nuspire

Second Annual CISO Research Report on Challenges and Buying Trends: A Focus on Optimization

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

nuspire.com

Table of Contents

```
import os, json, uuid, time
from datetime import datetime

from flask import Flask, render_template, request,
from flask_cors import CORS
import requests
from requests.auth import HTTPBasicAuth
from psycopg2_contextmanager import database_connection
import boto3

from auth import login_required

app = Flask(__name__)
app.config.from_object('config')
CORS(app)

lambda_client = boto3.client('lambda', region_name='us-east-1')

GS_API_URL = os.environ['GS_API_URL']
DATABASE_URL = os.environ['DATABASE_URL']
JOB_INGESTION_LAMBDA_NAME = os.environ['JOB_INGESTION_LAMBDA_NAME']


@app.route('/')
def serve_react_app():
    return render_template('index.html')

@app.route('/login', methods=['POST'])
def login():
    request_json = request.get_json()
    email = request_json.get('email')
    password = request_json.get('password')
    api_auth_endpoint = '{}v1/auth/'.format(GS_API_URL)
    auth_response = requests.get(api_auth_endpoint, auth=HTTPBasicAuth(email, passwo
    excluded_headers = ['content-encoding', 'content-length', 'transfer-encoding', '
    auth_response_headers = [(name, value) for (name, value) in auth_response.raw.he
```

Introduction

Understanding the challenges faced by chief information security officers (CISOs) and IT decision-makers (ITDMs) is critical for businesses looking to strengthen their cybersecurity posture, stay competitive and ensure regulatory compliance. It can also provide valuable insights for vendors looking to build partnerships and develop targeted solutions.

In its *Second Annual CISO Research Report on Challenges and Buying Trends**, Nuspire surveyed 200 CISOs and ITDMs to discover their pain points, priorities, budgets and motivations, as well as assess trends in their cybersecurity spending. What's unique about this report is that it also charts how CISO/ITDM challenges and priorities have evolved since the first report was published in August 2022.

Key Findings

The study found that CISOs/ITDMs continue to be most occupied with business, IT and security program strategy, but they are spending less time on threat research, awareness and hunting compared to 2022. The ever-evolving cybersecurity landscape and end-user error and education remain the biggest challenges for CISOs/ITDMs, with end-users accounting for much of their worries, specifically malware/ransomware, phishing and cloud security breaches.

CISOs/ITDMs report increased confidence in their cybersecurity systems, especially considering their security strategy relative to peers and end-user compliance. While many still feel their organizations are vulnerable to attack, concern is down slightly compared to last year.

Senior leaders continue to be highly involved and knowledgeable about the importance of cybersecurity measures, which could contribute to why CISOs/ITDMs indicated plans to increase overall cybersecurity spending despite recent economic trends and a looming recession.

Key Survey Findings

10% of CISOs and ITDMs manage all of their cybersecurity needs in-house

42% of CISOs/ITDMs say that their budget for cybersecurity has increased and that their spending will follow, despite recent economic trends pointing toward a recession

CISOs/ITDMs with <$1 million for outsourcing are more likely not to outsource compared to their peers with larger budgets (16% vs. 7%)

CISOs/ITDMs report increased confidence in their cybersecurity systems, especially thinking about their security strategy relative to end-user compliance (up 13 points) and peers (up 12 points)

They are now more concerned with software applications (up 7 points) and email/collaboration tools (up 5 points)

The unique challenges and IT pressures of remote work have fizzled out from the benchmark study, making way for greater emphasis on attracting and retaining skilled cybersecurity professionals

What Makes This Research Compelling?
Duo™ MaxDiff

Nuspire 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 choose 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 greater differentiation, which leads to more actionable results
- Helps identify the order and magnitude of results across a quadrant of dimensions

Top CISO Challenges

CISOs and ITDMs generally feel confident about their cybersecurity programs and strategy, but challenges persist.

Adapting to the Ever-evolving Cybersecurity Environment

Consistent with last year, CISOs/ITDMs' greatest challenges include adapting to the rapid rate of change within the cybersecurity landscape.

Sixty percent (down 7 points) of respondents believe their companies are somewhat vulnerable or extremely vulnerable to attack, which we infer points to a focus on strengthening protection against cyberattacks, particularly cloud applications, email/collaboration tools and software applications.

"The biggest challenge is trying to remain current on all the rapidly changing security risks."

Within digital environments, cloud applications are identified by 40% (down 2 points) as the most susceptible to attack, followed by email/collaboration tools at 40% (increase of 5 points), software applications at 40% (up 7 points) and cloud infrastructure at 38% (down by 1 point). When looking at 2022 data, end users and endpoints are no longer as concerning to CISOs/ITDMs.

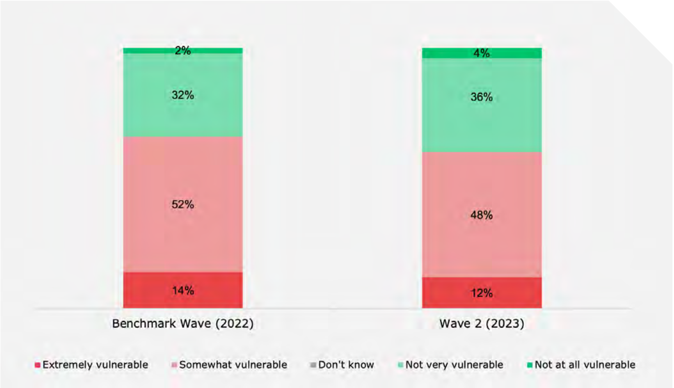


FIGURE 1: VULNERABILITY OF ORGANIZATION TO CYBERATTACKS
Showing % by wave

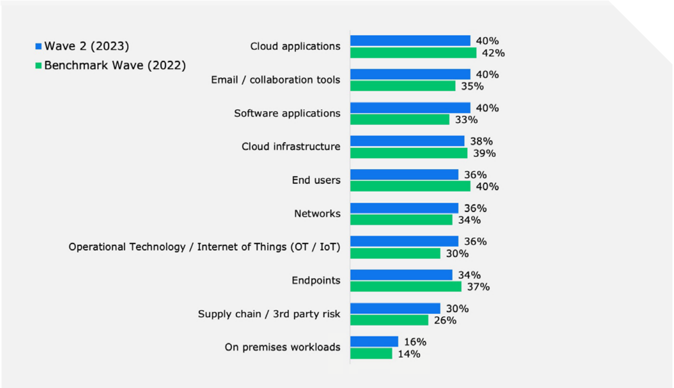


FIGURE 2: ASPECTS OF DIGITAL ENVIRONMENT THAT ARE MOST SUSCEPTIBLE TO CYBERATTACKS
Showing % by wave, ranked by Wave 2

"I would say the biggest challenge is the constantly changing and evolving nature of cybersecurity concerns. Hackers and cyber criminals are getting more and more sophisticated in their attacks."

Senior Leadership Engagement

In the not-too-distant past, CISOs and ITDMs lamented a lack of knowledge or engagement among senior leadership, making it more difficult to get buy-in and support for their initiatives. The research shows this issue diminishing, as 94% reported their senior leadership was very or somewhat involved in ensuring cybersecurity measures are up to date with the needs of their organizations. Similarly, 94% indicated that senior leadership was very or somewhat knowledgeable about the importance of cybersecurity measures.

Cybersecurity has firmly established itself as a business issue that deserves the attention of leaders across the organization – and this will go a long way in supporting CISOs/ITDMs as they work to keep up with rapid changes in the cybersecurity landscape.

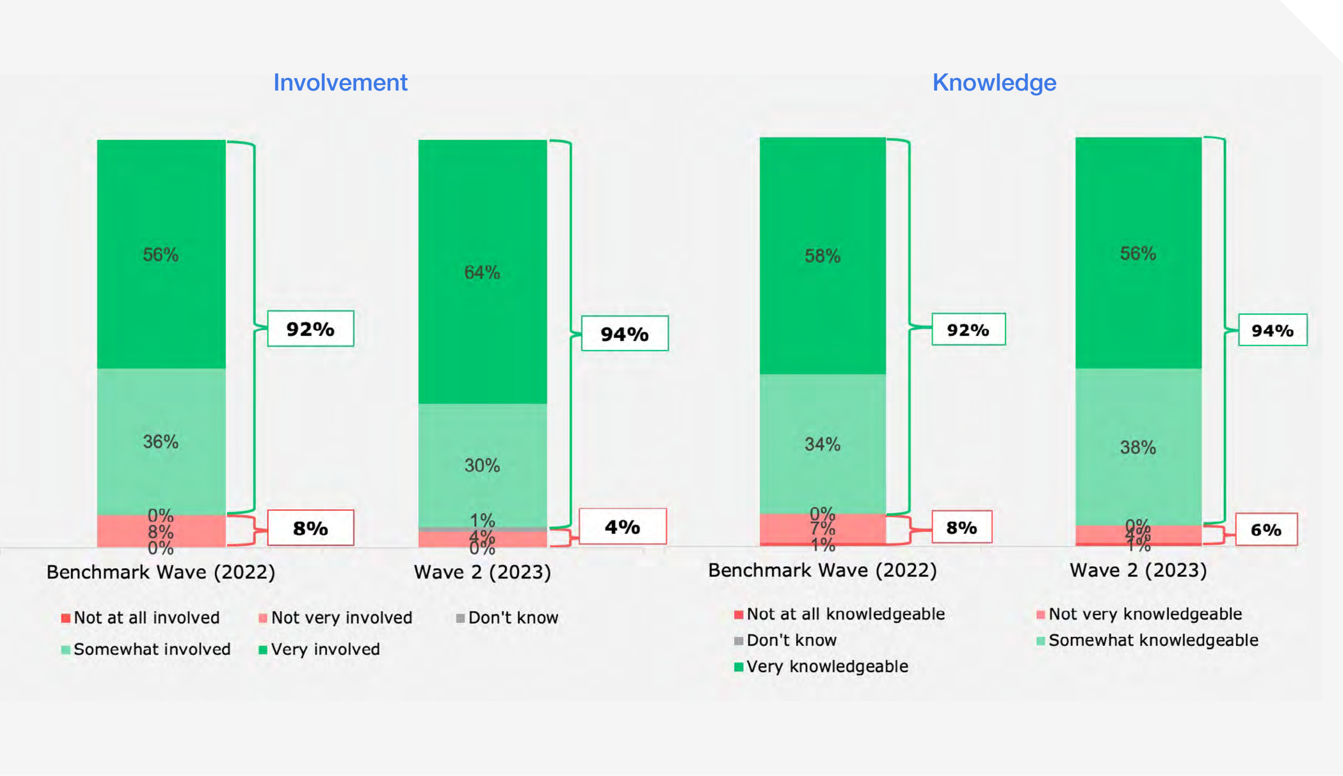


FIGURE 3: INVOLVEMENT & KNOWLEDGE OF SENIOR LEADERSHIP
Showing % by wave

Attracting and Retaining Highly Skilled and Better Trained Cybersecurity Professionals

This year, respondents placed greater emphasis on the **need to attract and retain cybersecurity professionals**, supplanting remote work concerns that topped the list in 2022. Talent shortages can create security vulnerabilities that can linger for weeks or months, increasing risk. Many threats aren't detected until an incident occurs.

- Sixty-six percent (no change) of respondents say it's hard to attract and retain qualified cybersecurity professionals.
- Fifty-eight percent (up 2 points) say their team is so busy, they might not detect an attack.
- Thirty percent of respondents say upgrading and enhancing cybersecurity skills would have the biggest impact on their security programs. Though down four points from 2022, this continues to be the enhancement most cited by respondents.

To alleviate the skills shortage, many organizations rely on outsourcing. You'll find more specifics on outsourcing later in this report.

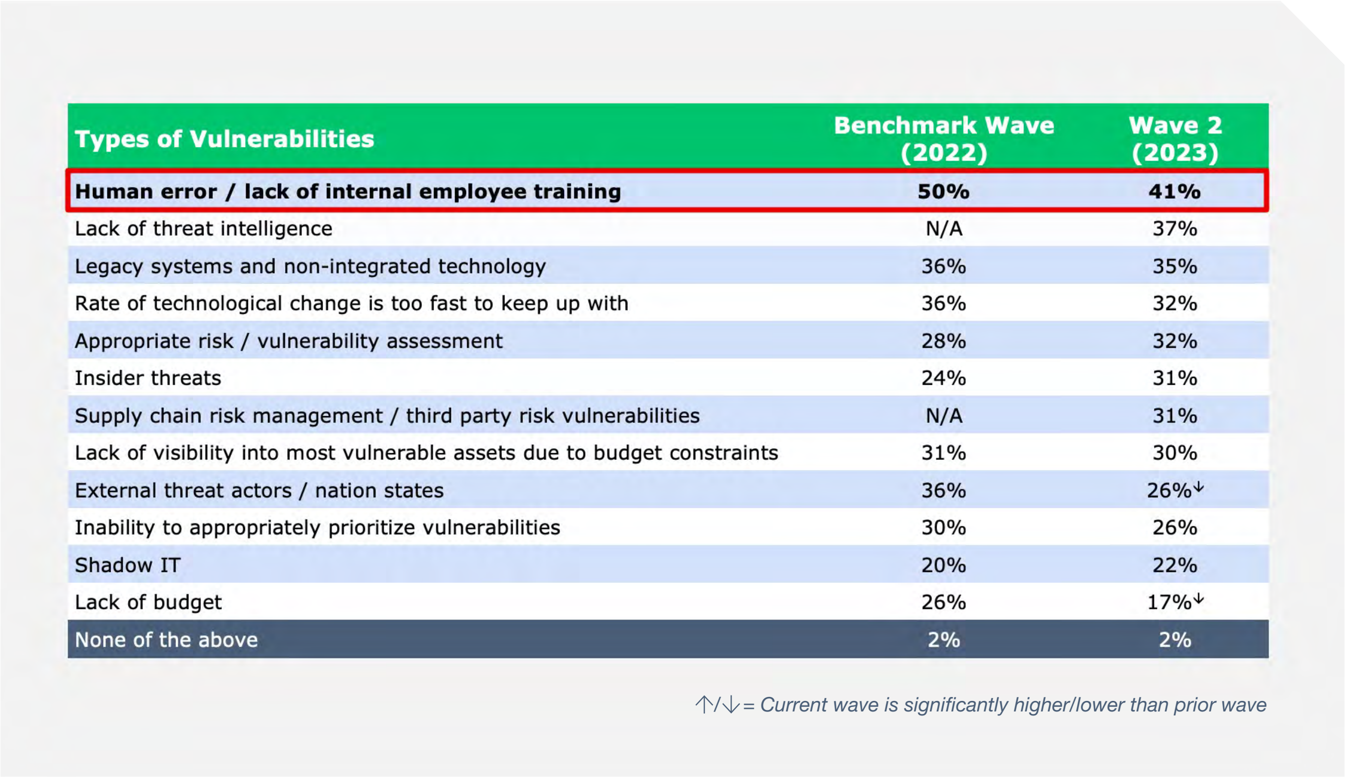
> "Recruiting and retaining talented security personnel is probably the biggest challenge at the moment for our company."

> "We are having challenges with finding the correct talent. The threats are constantly changing, and we must keep abreast of these threats."

Educating End-user Employees to Avoid Attacks

Employees are often the first line of defense against cyberattacks. Without proper training, they may not recognize the signs of malware and ransomware, phishing and cloud security breaches – cited by study participants as their most worrisome threats.

Human error and lack of internal employee training remains the No. 1 IT system vulnerability at 41% (down 9 points). Regarding the high-risk departments, IT, finance and accounting, and sales/marketing and human resources topped the list again this year. These departments are targeted by threat actors hoping to access IT servers, sensitive customer/vendor data and email accounts.



Types of Vulnerabilities	Benchmark Wave (2022)	Wave 2 (2023)
Human error / lack of internal employee training	**50%**	**41%**
Lack of threat intelligence	N/A	37%
Legacy systems and non-integrated technology	36%	35%
Rate of technological change is too fast to keep up with	36%	32%
Appropriate risk / vulnerability assessment	28%	32%
Insider threats	24%	31%
Supply chain risk management / third party risk vulnerabilities	N/A	31%
Lack of visibility into most vulnerable assets due to budget constraints	31%	30%
External threat actors / nation states	36%	26%↓
Inability to appropriately prioritize vulnerabilities	30%	26%
Shadow IT	20%	22%
Lack of budget	26%	17%↓
None of the above	2%	2%

↑/↓ = Current wave is significantly higher/lower than prior wave

FIGURE 4: MAIN REASONS FOR IT SYSTEM VULNERABILITIES
Showing % by wave, ranked by Wave 2

CISO Buying Trends

A Look at the Current State of Cybersecurity Budgets

With recent economic trends pointing toward a recession, experts expected to see a majority of respondents reporting budget reductions. However, the research reveals data to the contrary. Fifty-eight percent said their budgets had increased, and of those, 42% said they have plans to increase their budgets even more.

When asked about their company's investment in cybersecurity, CISOs/ITDMs generally believe they exceed their peers, in line with the last wave.

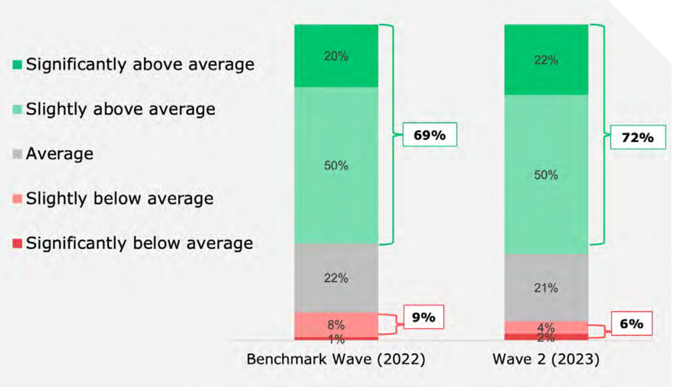


FIGURE 5: INVESTMENT IN IT/CYBERSECURITY RELATIVE TO PEERS
Showing % by wave

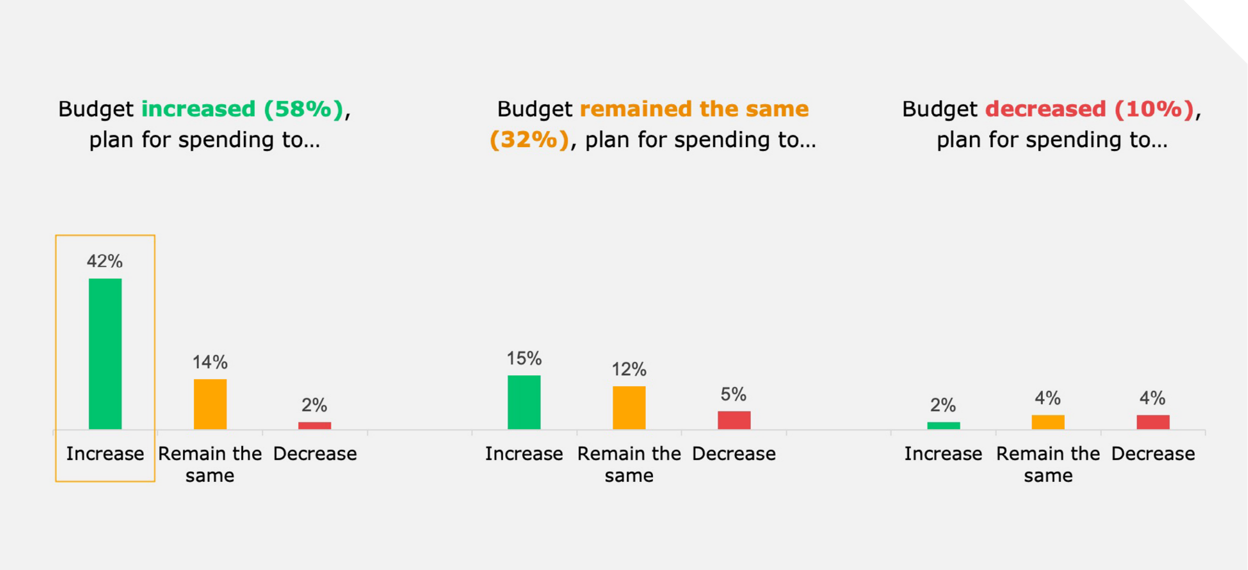


FIGURE 6: RECENT ECONOMIC TRENDS IMPACT
Showing % (only asked in Wave 2)

Budget size/experience correlates to likelihood to outsource

CISO and ITDM spending can vary by organization, but one interesting trend identified was the correlation between the size of the budget for outsourcing and the likelihood of a company to spend that budget on outsourced technologies or services. CISOs/ITDMs with less than $1 million for outsourcing were more likely NOT to outsource compared to their peers with larger budgets (16% vs. 7%). In addition, CISOs/ITDMs in their role for five or more years were also more likely NOT to outsource compared to more junior peers (15% vs. 5%).

A Focus on Maximizing Value

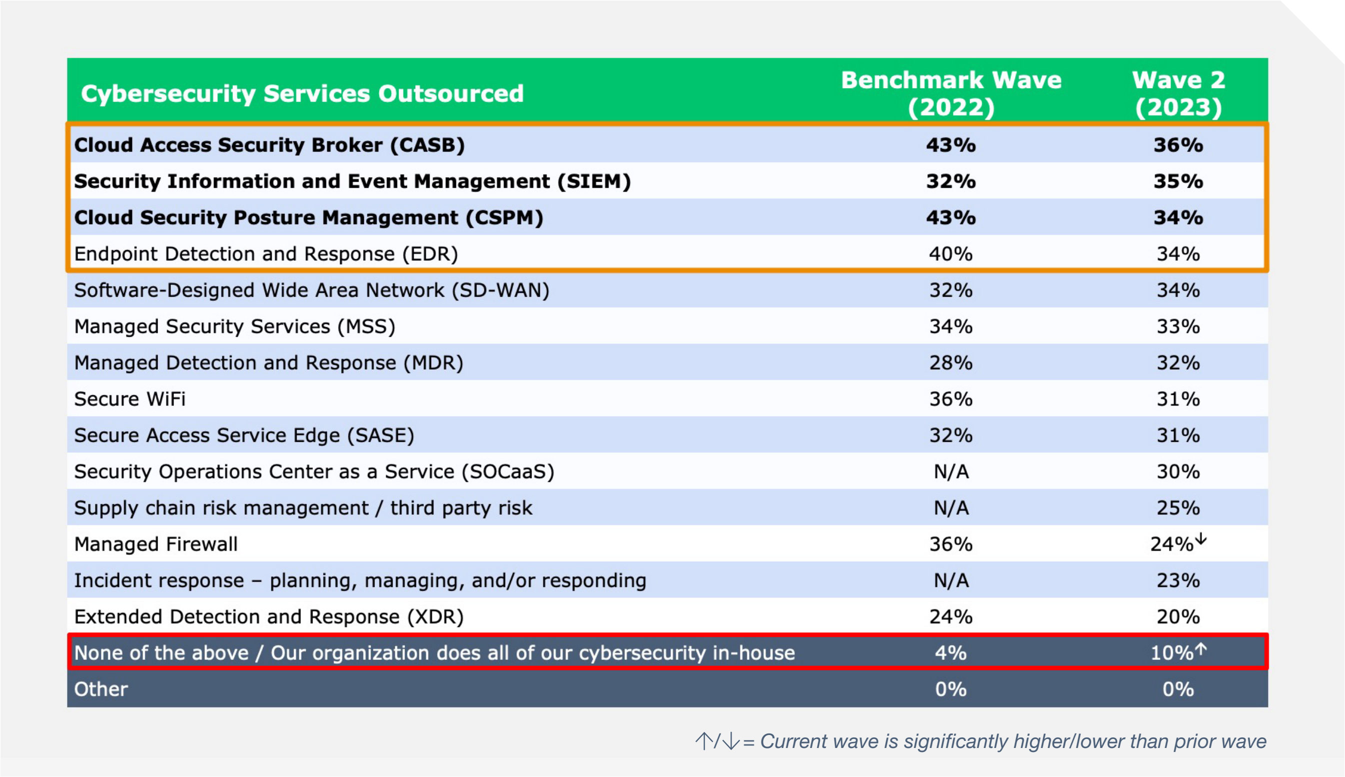
CISOs/ITDMs are split on what specific technology, skill or service would have the most significant impact on their organization's cybersecurity. However, the largest percentage (30%) say overall upgrades and enhancements would benefit their organization the most. This illustrates that an essential focus for CISOs/ITDMs is maximizing the value of their current cybersecurity investments.

That's not to say there won't be additional purchases of new technologies and services (see next section), but respondents indicate a desire to streamline and simplify. As one participant stated, "We have too many security tools. This is a big issue since we need to be experts at many tools."

Likelihood to Outsource: Top Security Program Must-Haves

The research reveals that, for the most part, the “must-haves” from last year still rank highly again this year. What has changed is the number of services in the “must-have” quadrant (see Figure 9). First, let’s highlight the top three “must-haves” (defined as services for which CISOs and ITDMs are willing to spend money), which remained the same from last year.

1. 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.
2. 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 7) are cloud access security broker (CASB) at 36% and security information and event management (SIEM) at 35%. Following closely at 34% includes cloud security posture management (CSPM), endpoint detection and response (EDR) and software-defined wide area network (SD-WAN).



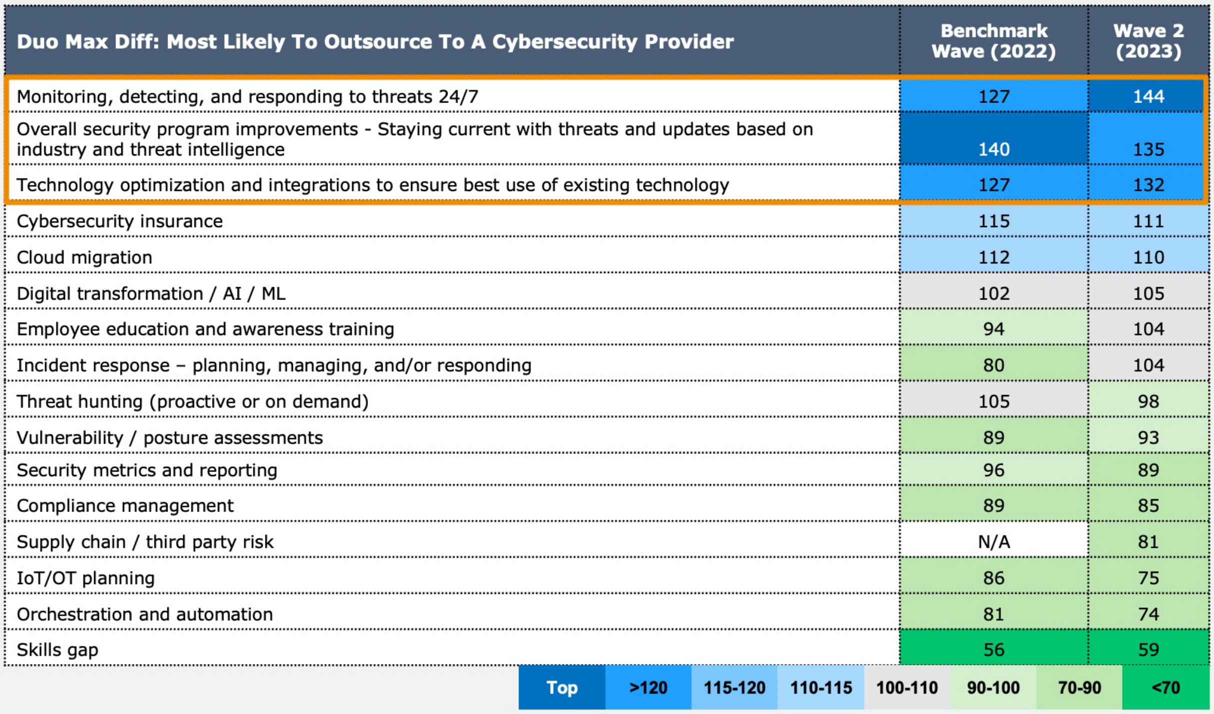
Cybersecurity Services Outsourced	Benchmark Wave (2022)	Wave 2 (2023)
Cloud Access Security Broker (CASB)	**43%**	**36%**
Security Information and Event Management (SIEM)	**32%**	**35%**
Cloud Security Posture Management (CSPM)	**43%**	**34%**
Endpoint Detection and Response (EDR)	40%	34%
Software-Designed Wide Area Network (SD-WAN)	32%	34%
Managed Security Services (MSS)	34%	33%
Managed Detection and Response (MDR)	28%	32%
Secure WiFi	36%	31%
Secure Access Service Edge (SASE)	32%	31%
Security Operations Center as a Service (SOCaaS)	N/A	30%
Supply chain risk management / third party risk	N/A	25%
Managed Firewall	36%	24%↓
Incident response – planning, managing, and/or responding	N/A	23%
Extended Detection and Response (XDR)	24%	20%
None of the above / Our organization does all of our cybersecurity in-house	4%	10%↑
Other	0%	0%

↑/↓ = Current wave is significantly higher/lower than prior wave

FIGURE 7: OUTSOURCED CYBERSECURITY SERVICES

Showing % by wave, ranked by Wave 2

3. Technology optimization and integrations to ensure the best use of existing technology. Few decision-makers opt for rip-and-replace solutions given budget constraints, so they look for assistance to determine how to maximize the efficacy of the tools they already have. This is where managed security services providers (MSSPs) are helpful because they can take stock of current assets, explore risk tolerance and ensure you can make every dollar count.



Duo Max Diff: Most Likely To Outsource To A Cybersecurity Provider	Benchmark Wave (2022)	Wave 2 (2023)
Monitoring, detecting, and responding to threats 24/7	127	144
Overall security program improvements - Staying current with threats and updates based on industry and threat intelligence	140	135
Technology optimization and integrations to ensure best use of existing technology	127	132
Cybersecurity insurance	115	111
Cloud migration	112	110
Digital transformation / AI / ML	102	105
Employee education and awareness training	94	104
Incident response – planning, managing, and/or responding	80	104
Threat hunting (proactive or on demand)	105	98
Vulnerability / posture assessments	89	93
Security metrics and reporting	96	89
Compliance management	89	85
Supply chain / third party risk	N/A	81
IoT/OT planning	86	75
Orchestration and automation	81	74
Skills gap	56	59

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

FIGURE 8: MOST LIKELY TO OUTSOURCE TO A CYBERSECURITY PROVIDER

Three services have jumped to the "must-have" quadrant:

- Cybersecurity Insurance: In 2022, respondents indicated they were likely to outsource cybersecurity insurance, but it wasn't high on the list in terms of concern. This year, however, cyber insurance has shot over to the upper right-hand quadrant in Figure 9. While this doesn't definitively pinpoint the reason, 2023 trends reveal more stabilization within the cyber insurance industry. The skyrocketing rates in 2021 and 2022 are starting to slow, the underwriting process is improving, and organizations feel better prepared to adhere to policies' stringent requirements.
- Employee Education and Awareness Training: This jumped from a relatively low concern and likelihood to outsource (the "less urgent" quadrant in Figure 9) last year to the top right quadrant as a "must-have" this year. Why? Last year, organizations prioritized other areas on which to focus, believing they could manage education and training in-house.
- Incident Response – Planning, Managing and/or Responding: IR also jumped from the "less urgent" to the "must-have" quadrant. Cybersecurity talent shortages and an increase in cyberattacks are requiring CISOs to augment internal IR resources.

The services in the "less urgent" quadrant include:

- Orchestration and Automation: Orchestration and automation stayed relatively the same as last year. Perhaps this is due to organizations already having technology and services in place to address this issue.
- IoT/OT Planning: IoT/OT attacks continue to rise, yet results from the study show this area is a low area of concern and not something CISOs/ITDMs plan to outsource. Organizations may feel they have sufficient defenses like EDR or MDR to combat these types of attacks.
- Security Metrics and Reporting: Metrics and reporting are critical to a successful security program; however, it remains in the "less urgent" quadrant. The reason could be attributed to what we see in Figure 3. With knowledgeable and involved leadership, CISOs/ITDMs can get what they need with internal reporting capabilities.

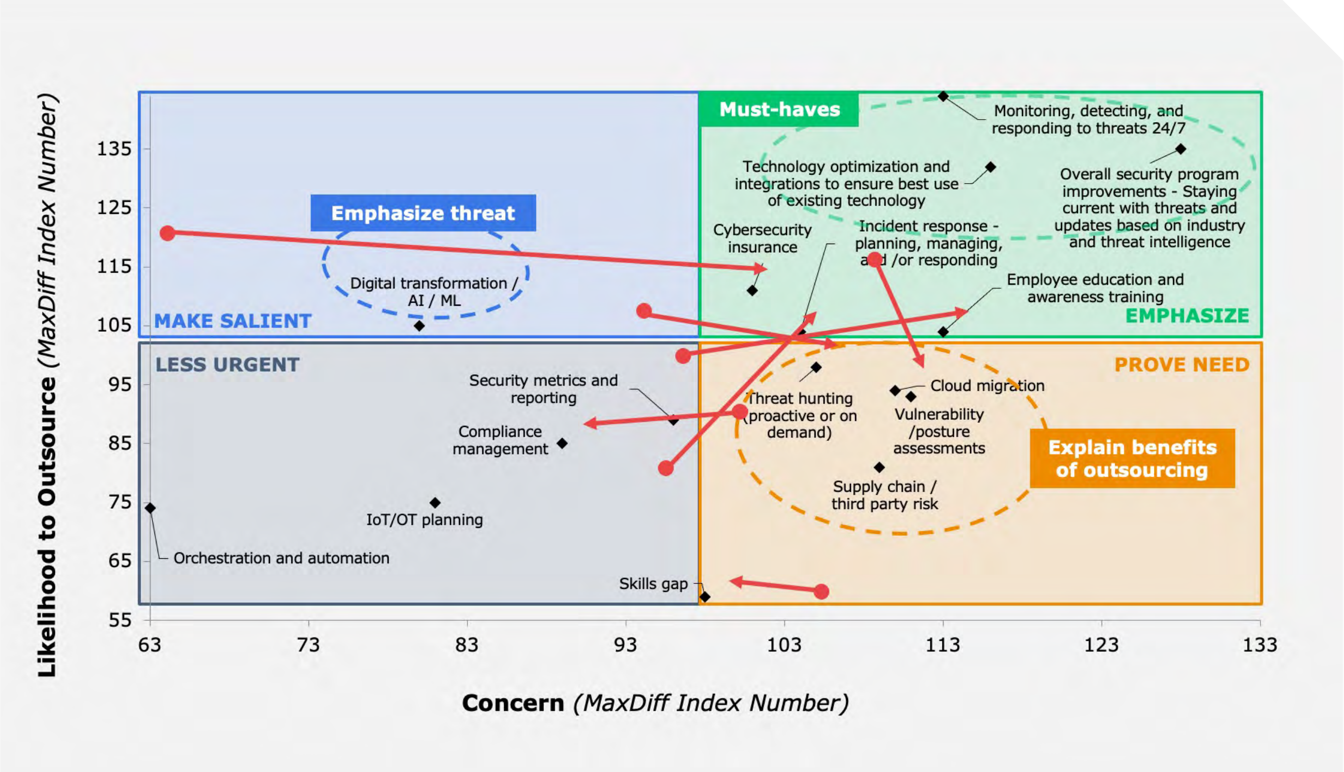


FIGURE 9: DUOMAXDIFF SHOWING CONCERN AND LIKELIHOOD TO OUTSOURCE

Red arrows represent movement between quads from benchmark

Buying Trends Suggest a Focus on Optimization

While CISOs and ITDMs have a relatively high level of confidence in their current cybersecurity programs, it’s clear that the pressures to mitigate risk are growing. Leaders across departments now recognize cybersecurity’s importance to their bottom line, and that heightened interest creates increased pressures on security practitioners to deliver.

As revealed in Figure 9, the number of solutions CISOs and ITDMs consider crucial to their business has grown. With indications that budgets are increasing, security leaders are spending more time on optimization to determine the following:

- The best solutions for detecting and responding to cyberattacks. The lack of skilled cybersecurity professionals remains a top concern, and CISOs and ITDMs are purchasing solutions that directly address threats.
- The levers they can pull to extract the most value from their security investments.
- Prevention measures to stop adversaries earlier in the cyber kill chain.

Remote work, once considered a five-alarm fire in the security world, has become business as usual, giving CISOs and ITDMs time and resources to evaluate the performance of their entire security tech stack. It’s no longer about purchasing the new, shiny security innovation, but rather inventorying existing assets and figuring out how to ensure those assets are protecting the organization’s most important information and processes.

And when there are gaps, CISOs and ITDMs purchase the technologies and services that most directly address pressing needs and have a track record of performing well, i.e., MDR, incident response and expert support such as managed security services providers (MSSPs).

**Unless otherwise noted, stats and findings come from Nuspire research (n=200, CISOs and ITDMs in the U.S. representing 14 industries and companies ranging from 500 to 10,000+ employees) conducted in Q1 2023. A Duo™ MaxDiff approach was used to analyze the data.*

nuspire

About 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