ARCTIC WOLF

Trends Report 2025

Table of Contents

Foreword

The past year was a busy one for IT and security leaders. On top of the usual responsibilities and everyday threats, security teams grappled with the continued emergence and adoption of transformative AI technologies, an evolving and uncertain regulatory climate, rising global tensions, as well as arguably the largest IT outage in history.

The Arctic Wolf State of Cybersecurity: 2025 Trends Report is an opportunity for decision makers to share their experiences over the past 12 months and their perspectives on some of the most important issues shaping the IT and security landscape.

Our research reveals that ransomware continues to be a perennial area of concern, but for the first time in four years, it isn't the top concern for IT and security leaders. **This year, AI ranks at the top of the list as indicated by 29% of respondents, relegating ransomware to second place.**

The percentage of organizations reporting being victim to a ransomware attack also declined with **23% of respondents disclosing that their organization experienced at least one "significant" ransomware attack in 2024, compared to last year's response of 45%.**

While the reduction in ransomware attacks is positive news, still **70% of security leaders polled report that their organization experienced at least one "significant cyber attack" in 2024.**

It makes sense then that in response to growing attacks, IT and security leaders are actively preparing to respond to incidents, with **88% of organizations having purchased an active incident response (IR) retainer.**

The large adoption of IR retainers points to a trend in recognizing the necessity of having risk transference measures at the ready in the face of crisis. However, when examining respondents' adoption and usage of risk mitigation solutions, a less uniform and overall, less positive picture emerged.

Despite the broad adoption of next-generation endpoint security solutions, visibility gaps remain. Additionally, **nearly a quarter of those polled report outright dissatisfaction with an element in their security stack, citing high rate of false positives (34%) and lack of efficacy (33%) as their top challenges.**

Looking ahead, data transformation and AI adoption is the most frequently cited driver of cybersecurity investments for the coming year, yet conversely, **18% of security leaders indicate that AI devices delivered the least amount of value in the past year.**

While the current level of AI exuberance feels at direct odds with limited security outcomes AI investments have delivered to date, integrating AI into a proven solution to augment the broader set of people, processes, and technologies provides more upside than operating under the expectation that entire security functions can be delivered by an AI engine.

Ultimately, the hype around AI may distract from more important — and more effective — security investments, many of which are far more mundane, yet far more impactful in maximizing positive security outcomes.

As you review the report and accompanying analysis, our hope is that the insights provided help you and your organization improve resilience in the months and years ahead.

LISA TETRAULT,
Senior Vice President,
Security Services

Methodology

The survey was conducted among 1,200 IT and security decision makers at director level or above, from organizations with 50+ employees, across the U.S., U.K., Canada, ANZ (Australia, New Zealand), DACH (Germany, Austria, Switzerland), the Nordic regions (Norway, Sweden, Denmark, Finland), Benelux (Belgium, the Netherlands, Luxembourg), and South Africa, during January and February 2025.

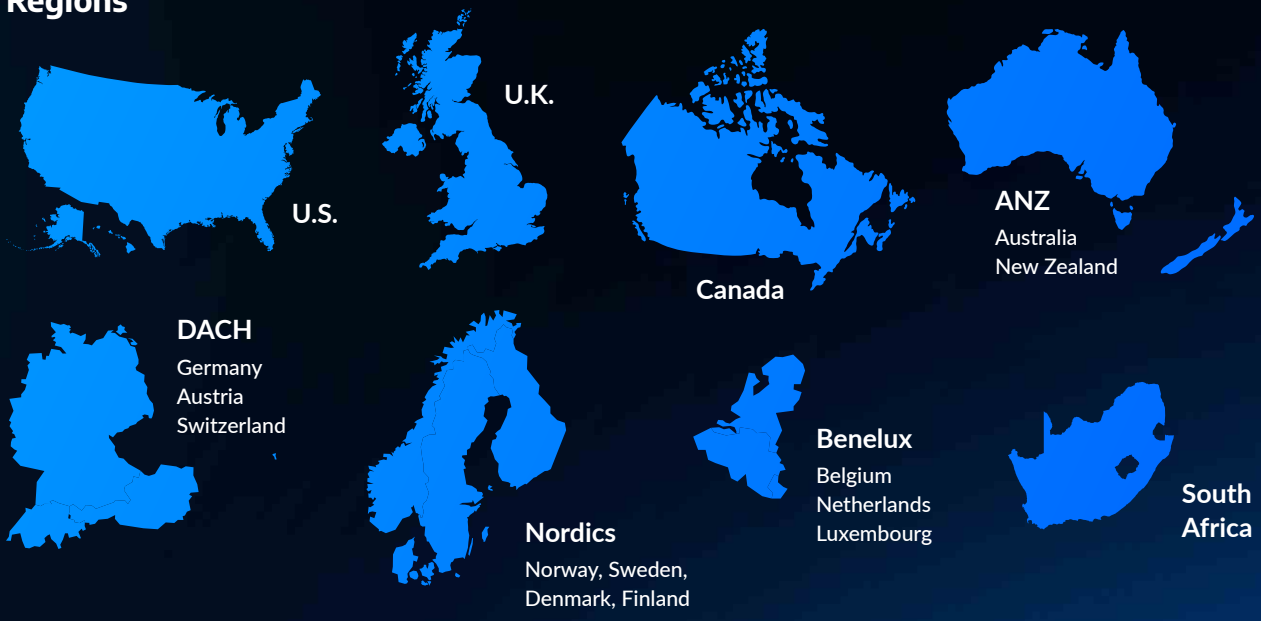
Respondents

46%
Director or Vice President

36%
C-Level Executive

19%
Owners

Regions



95 in 100 In this particular study, the chances are 95 in 100 that a survey result does not vary, plus or minus, by more than 2.8 percentage points from the result that would be obtained if interviews had been conducted with all persons in the universe represented by the sample.

Regional Trends: EMEA

EMEA

GLOBAL

IRELAND

Organizations in Ireland were the least likely to maintain an active IR plan to respond to threats when they occur.

Across the full respondent population, 60% of organizations maintain an active Incident Response (IR) plan — yet in Ireland only 30% of organizations are prepared with an up-to-date IR plan.

NORDICS

GLOBAL

More than half (51%) of respondents from the Nordics (Denmark, Finland, Norway, and Sweden) reported that their organization suffered a BEC attack — 16% higher than the global average.

This is plausibly due to the prevalence of banking and finance services companies, as our threat research regularly shows BEC threat actors target organizations in the financial sector.

GLOBAL

U.K.

Good backup practices led to only 13% of respondents from the United Kingdom citing a lack of sufficient backups as the reason why their organization paid a ransom — one third of the global rate (39%).

With reliable backups, why are victims in the U.K. still choosing to pay the ransom? We found 60% — 11% above the global average — electing to pay to speed up recovery.

Regional Trends: ANZ

ANZ

INTELLECTUAL PROPERTY, DATA, AND PRIVACY PROTECTION

Respondents from Australia and New Zealand reported intellectual property, data, and privacy protection as the main driver of their security strategies,

while AI Adoption drives strategies for the rest of the globe.

Organizations in Australia and New Zealand were 9% more likely to suffer a "significant" cyber attack than the global average (85% versus 76%).

Consistent with their top driver of security strategy,

74% of victimized organizations in Australia and New Zealand that paid a ransom did so to prevent the release of stolen data — well above the global average of 50%.

Regional Trends: North America

NA

CANADA

GLOBAL

Organizations in Canada are taking a more measured and apprehensive approach to emerging technologies than those in other nations,

with 40% of respondents from Canada reporting that their organization has already implemented policies totally banning the usage of generative AI and LLMs (ChatGPT), compared to a 30% global average.

UNITED STATES

When asked about cybersecurity budgets, 18% of respondents from the United States felt their organization was incorrectly investing their budgets and creating an imbalance,

either by overspending on technology that was being underutilized, or by overspending on expertise to the detriment of technology investments.

GLOBAL

UNITED STATES

CANADA

Organizations in Canada appear may be understaffing their security programs.

Of all the countries polled, respondents from Canada were the least likely to indicate that their organization had adequate staffing, with only 36% doing so — compared to 48% in the United States and 50% globally.

SECTION 1

Threat Trends

TREND 1

AI Emerges as the Leading Cybersecurity Concern

Security leaders have a lot to worry about. Headlines and security alerts offer near-constant reminders that the threat environment is always evolving. At the same time, each and every organization's security posture is always in a state of flux.

Given such a dynamic context, it's always revealing to discover what security leaders consider to be their primary area of concern.

This year, we have a new 'winner,' with "AI, large language models (LLMs), and associated privacy concerns" chosen by 29% of respondents.

What is your primary area of concern when it comes to cybersecurity in general? *(select one)*

Plan for the future, but don't overlook the present

In taking the top spot, AI relegates longtime leading concern ransomware to second place (21%).

It's encouraging that security leaders take the threats associated with AI very seriously. However, it is important to remember that while AI has the ability to automate, accelerate, and enhance attacks, whether that's crafting more convincing phishing emails or more easily identifying system vulnerabilities, AI is the tool by which threats are being delivered and enhanced but, AI is not the threat itself.

A real risk with AI's novelty and hype is that it is distracting from genuinely larger risks. For example (as we'll see a little later), the survey revealed that many organizations experienced ransomware or business email compromise (BEC) attacks. Plus, the Arctic Wolf 2025 Threat Report showed that ransomware and BEC attacks aren't mere inconveniences —they account for 44% and 27%, respectively, of incident response (IR) cases investigated by Arctic Wolf.

Similarly, identity is becoming a major battleground in modern cybersecurity, and today's threat actors are adept at finding and leveraging credentials that allow them to log into services and move unnoticed around victim environments. Moreover, attackers routinely employ social engineering and take advantage of misconfigurations to pursue their objectives.

The challenge for security leaders is to simultaneously develop and implement plans to safeguard against emerging threats without downplaying or overlooking those that are all too real today.

TREND 2

Breaches Remain All Too Common, and Disclosure Obligations Are Forcing Transparency

In a cybersecurity context, a data breach is an incident in which one or more unauthorized parties access computer data, applications, networks, or devices.

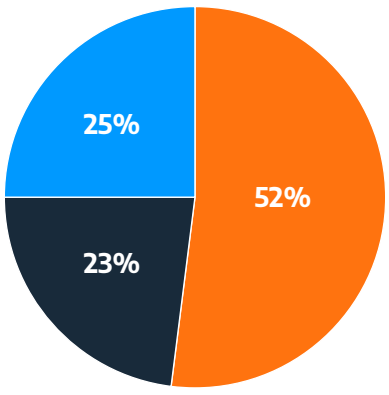
Unfortunately, such incidents remain all too common. The survey responses indicate that in the last 12 months, 52% of organizations identified one or more breaches within their environment (up from 48% a year ago).

But the story doesn't end there, as an additional 23% of respondents conceded that they were unsure if a breach had occurred. In other words, they lacked sufficient visibility and detection capabilities to rule out the possibility.

Flipped around, these findings reveal that **only 25% of security leaders can say with any confidence that their organization had not suffered a breach in the last 12 months** — a significant decrease over last year (35%).

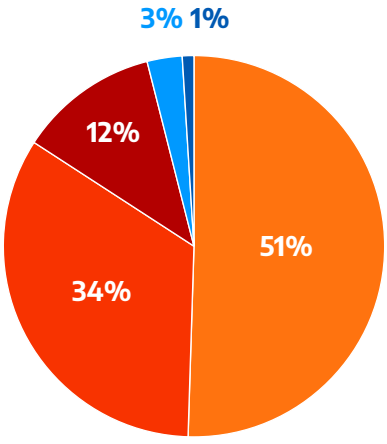
Of those organizations that knew with certainty they had been victimized, 97% disclosed the breach (consistent with last year's 96%). This high rate of disclosure is due mostly to obligations: 51% of respondents reported disclosing due to a legal requirement to do so, while a further 34% cited a requirement from either an insurance provider or other outside entity.

In the last 12 months, has your organization suffered a breach? *(select one)*



- Yes, we are certain a breach has occurred
- Possibly, we are unsure whether a breach occurred
- No, we are certain a breach hasn't occurred

Did your organization disclose the breach? *(select one)*



- Yes, we are required by law
- Yes, as required by our insurance provider or another outside entity
- Yes, to share our findings with the broader security community
- No, we were legally prevented from doing so
- No, for fear of brand damage

TREND 2

Breaches Remain All Too Common, and Disclosure Obligations Are Forcing Transparency continued

Security leaders adopt a more realistic perspective

There are two ways to look at the key finding that only a quarter of respondents are confident their organization didn't suffer a breach (and it's likely there's some truth in each).

The pessimistic view is that despite continued spending on cybersecurity, confidence is decreasing. This speaks to an observation that Arctic Wolf has made time and again: that cybersecurity has an effectiveness problem.

The optimistic view is that security leaders have considerably less misplaced confidence than in years past. In other words, leaders are adopting more realistic perspectives on the difficulty of detecting breaches. This shift may be informed by past experiences, like the famous SolarWinds supply chain compromise that forced many organizations to come to terms with the fact they had been breached for months without being aware of the fact.

For additional context, more than 62% of initial Arctic Wolf deployments reveal one or more latent threats (a hidden or dormant risk within an environment that hadn't been detected by the organization's existing security measures).

As noted above, the sustained high rate of disclosure is due mainly to obligations. For readers in the United States, it's worth noting that even though there's some uncertainty around the future of federal-level regulation, many states have passed their own disclosure laws. Plus, we can reasonably expect insurers to continue to require disclosure as part of the claims process.

But let's take a moment to tip our caps to the 12% of organizations that made the admirable decision to disclose simply to share their findings with the broader security community. We're all in this fight together, and such selfless transparency — despite the potential negative consequences of doing so — is a rising tide that lifts the cybersecurity community.

62%

More than 62% of initial Arctic Wolf deployments reveal one or more latent threats.

(a hidden or dormant risk within an environment that hadn't been detected by the organization's existing security measures).

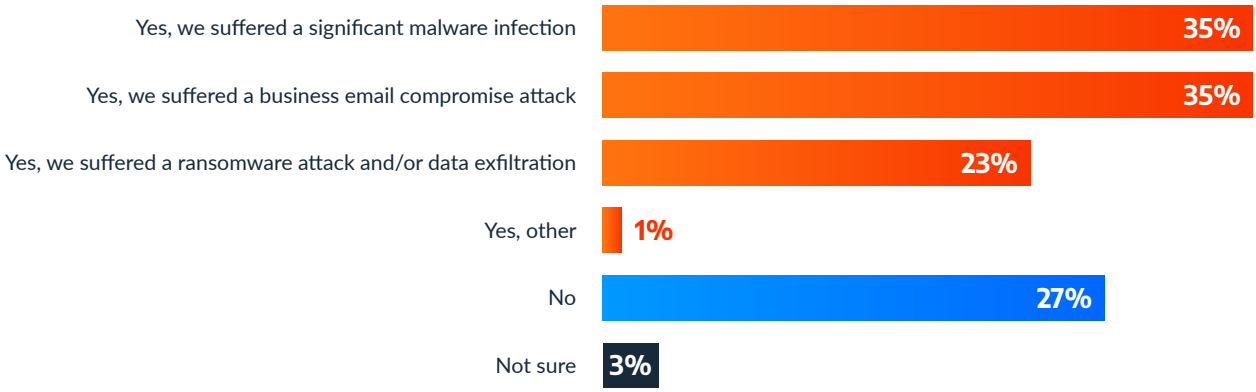
TREND 3

Significant Cyber Attacks Continue, with Lasting Consequences

Looking beyond the subset of incidents that qualify as breaches, 70% of security leaders polled reported that their organization experienced at least one "significant cyber attack" in 2024.

The most common incidents were malware infections and business email compromise. Both of these threats were reported by 35% of respondents, outpacing ransomware and/or data exfiltration (23%).

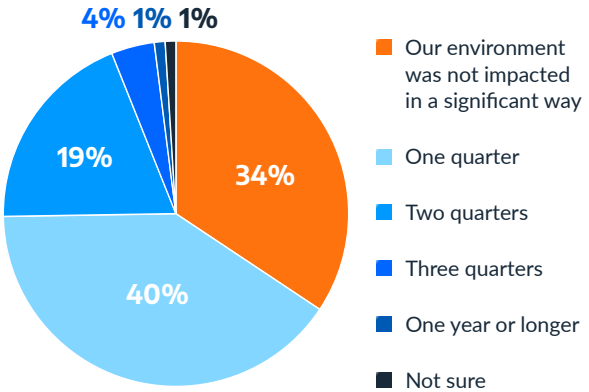
Did your organization experience a significant cyber attack in 2024? *(select all that apply)*



Nearly two thirds (64%) of the significant cyber attacks led to a loss of productivity lasting at least three months. This means that 45% of organizations, overall, experienced a cyber attack-imposed productivity loss lasting for at least one quarter in 2024.

And for some, the disruption lasted much longer: 24% of organizations that suffered a significant attack experienced productivity losses for six months or longer.

How long did your environment experience a loss of productivity, if at all? *(select one)*



TREND 3

Significant Cyber Attacks Continue, with Lasting Consequences continued

Preserving productivity requires prioritizing security investments

First, let's address an elephant in the room: more than half (56%) of the organizations that experienced a significant cyber attack had not implemented multi-factor authentication (MFA). Nowadays, strong phishing-resistant MFA (e.g., based on the FIDO2 set of specifications) should be regarded as a basic, fundamental, non-negotiable element of an organization's security posture. The MFA hurdle can help not only to stop attackers from gaining initial access, but also to thwart intrusion actions.

Second, let's return to the seeming disconnect first noted in Trend No. 1: that AI's security and privacy implications represent the leading cybersecurity concern, even though malware, BEC, and ransomware attacks are common occurrences leading to prolonged losses of productivity (among many other consequences). Perhaps we can reconcile these somewhat contradictory findings by pointing to human nature. After all, it seems plausible that security leaders are so familiar with these traditional attacks — and have some experience guarding against and recovering from them — that they seem more manageable compared to the still-emerging threats associated with AI.

Finally, the productivity losses underscore the importance of preparedness and prevention, which can only come by appropriately prioritizing cybersecurity investments. In other words, mature organizations should regard cybersecurity products, solutions, services, and capabilities — like MFA, for example — not as sunk expenses, but as investments to preserve continuity and protect productivity.

56% **More than half of the organizations that experienced a significant cyber attack had not implemented multi-factor authentication (MFA).**

TREND 4

Ransomware is Still a Major Problem, But Professional Negotiators Are Reducing Payouts

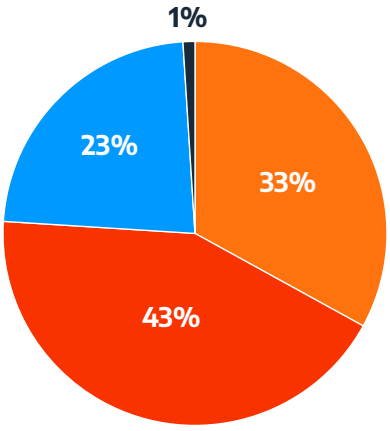
As shown previously, 23% of respondents reported that their organization experienced at least one "significant" ransomware attack in 2024.

Notably, this is substantially lower than the previous year (45%), although the higher figure may have been swelled by incidents that weren't deemed by the victims to be "significant."

More than three quarters (76%) of the organizations that experienced a significant ransomware attack elected to pay the ransom, down slightly from last year's figure (83%). Within this group, 43% of victimized organizations (33% overall) made the payment entirely from their own coffers, whereas 57% of victims (43% of organizations overall) received at least some funds from their insurance provider or another outside entity.

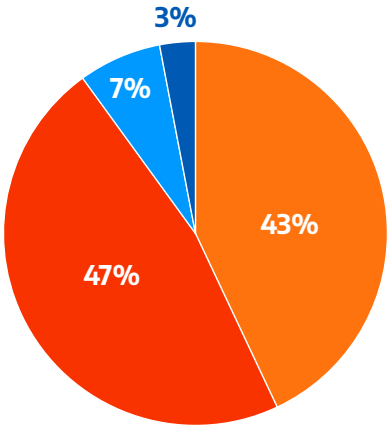
The overwhelming majority — fully 90% — of ransomware victims engaged the services of a professional ransomware negotiator. For more than half of those who went this route (52%), doing so led to a reduced ransom. In contrast, only 30% of organizations that handled negotiations themselves were able to secure a reduction.

Was the ransom paid? *(select one)*



- Yes, the ransom was paid by our organization only
- Yes, but the ransom was paid in some capacity by our insurance provider / outside entity
- No, the ransom was not paid
- Not sure

Did you hire or utilize a professional outsourced ransomware negotiator? *(select one)*



- Yes, but we were still required to pay the full demand amount
- Yes, and we only paid a portion of the demand
- No, and we paid the full demand amount
- No, and we only paid a portion of the demand

TREND 4

Ransomware is Still a Major Problem, But Professional Negotiators Are Reducing Payouts continued

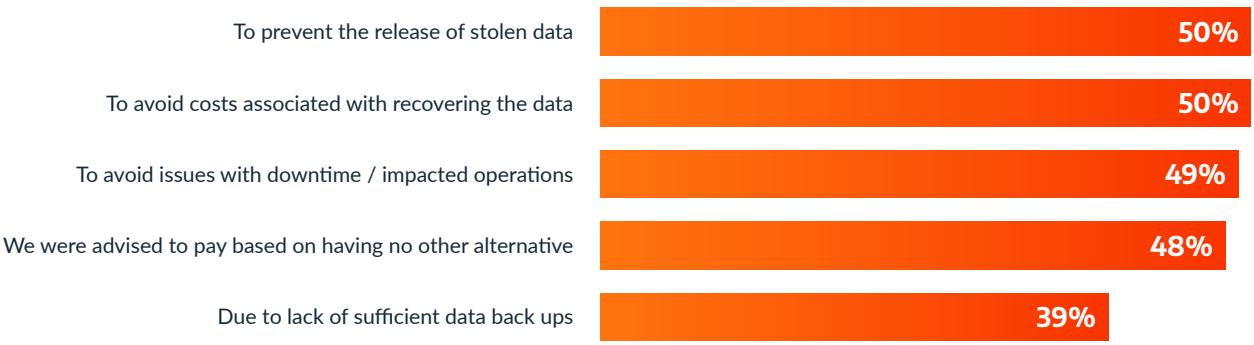
At a high level, there are three reasons why organizations elect to pay a ransom.

First, to prevent the release of stolen data. In 2019, the Maze ransomware operation exfiltrated sensitive data from Allied Universal and threatened to publish it unless the ransom was paid. Since then, the "double extortion" model has become the norm due to the pressure it exerts — including against victims with reliable backup and restoration processes — and half (50%) of victimized organizations cited this as their reason for paying.

Second, to make recovery faster, less expensive, or more complete. Even when backup and restoration processes are in place, paying the ransom may be considered — economically, at least — the prudent choice.

Third, because doing so offers the only available path to recovery. For obvious reasons, this is the worst case scenario. Unfortunately, the survey indicates that 48% of ransomware victims found themselves in this position.

Why did you pay the ransom? *(select all that apply)*



TREND 4

Ransomware is Still a Major Problem, But Professional Negotiators Are Reducing Payouts continued

Preparedness and professional negotiation pay off

The lower reported rate of ransomware attacks is consistent with other observations — including those shared within the **Arctic Wolf 2025 Threat Report** — that suggest some combination of decreased ransomware activity and increased resilience to such incidents. Notwithstanding these favorable signs, the ransomware landscape has seldom been noted for its constancy, so organizations shouldn't overlook the ongoing risk.

Shifting attention to ransom payments, we'll first note that Arctic Wolf's position aligns with the general recommendations of the FBI, other law enforcement agencies, and governments: if possible, ransom demands should not be paid, as starving the perpetrators is the only way we can collectively hope to eliminate these attacks.

Nevertheless, the decision on whether to pay is one that must be made by stakeholders within the victim organization once presented with all possible information and options.

While it's encouraging to see a year-over-year reduction in payment frequency, the 76% rate reported by this year's respondents — despite 90% of them working with a professional negotiator — is vastly higher than the 30% payment rate within Arctic Wolf Incident Response cases (covered in our **2025 Threat Report**). This disparity suggests that the capabilities of professional ransomware negotiators vary, and that it's worth working with the most experienced and skilled ones.

Finally, the survey results underscore the importance of proper back-up and restoration practices to increase resilience against ransomware attacks. While backups don't address the issues around data exfiltration, being able to restore business operations can buy your organization time and limit the ripple effects of the attack.

76%

The 76% pay off rate reported by this year's respondents is vastly higher than the 30% payment rate within Arctic Wolf Incident Response cases.

(covered in our **2025 Threat Report**)

SECTION 2

Mitigation Trends

TREND 1

Despite Widespread Adoption of Next-Generation Endpoint Security Solutions, Visibility Gaps Persist

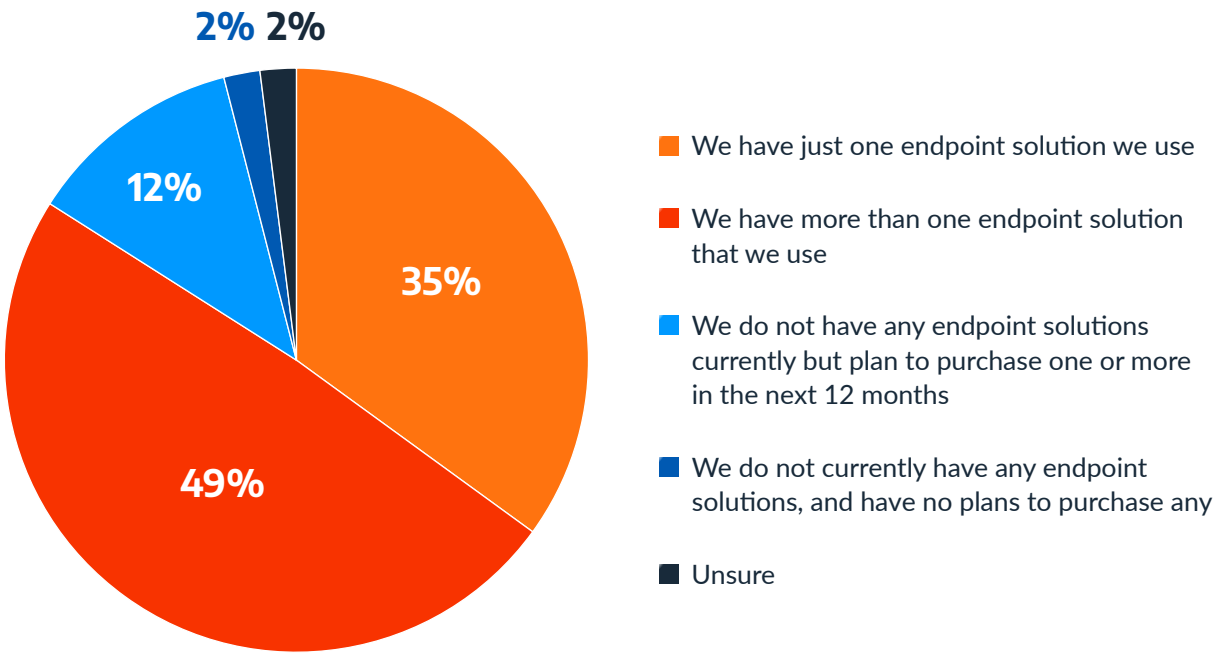
An endpoint is any physical device that resides at the end point of a network connection and can communicate on that network.

This includes (but is not limited to) desktops, laptops, servers, mobiles, workstations, and Internet of Things (IoT) devices.

Endpoints pose a difficult security challenge. The make and model of endpoints vary widely, as does the operating system, the apps or programs installed on them, and the security habits of each endpoint user. The rise of hybrid work has increased these challenges, as endpoints have become more portable than ever before.

The large majority of leaders polled (84%) indicated that their organization utilizes next-generation endpoint security solutions — including endpoint detection and response (EDR), endpoint protection platforms (EPP), or extended detection and response (XDR). In fact, nearly half (49%) have deployed two or more solutions. Of the 16% whose organizations don't yet have such a solution in place, three quarters (12% of respondents overall) noted that there are plans to purchase a solution in the next 12 months.

Does your organization currently utilize one or more next generation endpoint security solutions (EPP, EDR, XDR)? *(select one)*



TREND 1

Despite Widespread Adoption of Next-Generation Endpoint Security Solutions, Visibility Gaps Persist continued

Closing visibility gaps

A successful approach to endpoint security is one that includes visibility into any physical device that can transmit and receive data on your network. A lack of such visibility — including having too few signal sources — allows security threats to go unnoticed for far too long.

However, despite the broad adoption of next-generation endpoint security solutions, visibility gaps remain. Of those organizations that already have a solution deployed — and focusing only on desktops, laptops, and servers, while omitting IoT devices — only 40% of security leaders indicated that they have 100% coverage and expect to maintain that level in the future. By leaving gaps, those organizations are inviting risk.

It's also worth noting that an overreliance on a single endpoint security vendor can also lead to trouble — a point that became apparent in the wake of CrowdStrike's infamous July 2024 outage. While no vendor is immune to the potential for outages, whether they originate from attackers or internal misconfigurations, the CrowdStrike situation highlighted the critical need to eliminate single points of security failure.

To be ready for modern threats, it's essential to ensure you have the right people, processes, and technology in place to:

Continuously monitor your environment, even if a key technology or telemetry source goes offline

Collaborate with a diverse set of vendors to avoid over-reliance on a single platform

Develop a plan with your security partners for when things go wrong

Adopt a security operations approach to minimize your overall risk

TREND 2

Budgetary Pressures and Legacy Solutions Are Increasing Cyber Risk

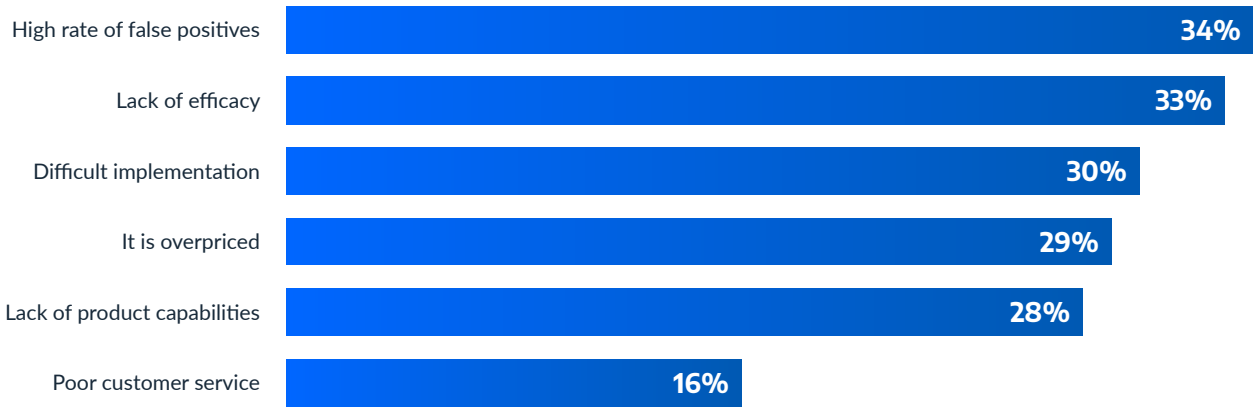
In an ideal world, cybersecurity solutions are procured based on careful evaluation of capabilities, in the specific context of the purchasing organization's IT environment, with decisions perhaps aided by input from trusted experts.

However, such a process doesn't always play out. For example, when asked why they chose their current endpoint tool, 49% of respondents indicated that it was bundled with other security tools they purchased, 32% cited the combination of low cost and limited budget, and 24% inherited a legacy solution.

And there's no reason to conclude that similar forces aren't influencing other cybersecurity purchase decisions. Perhaps that's why roughly a quarter (24%) of security leaders polled indicated that they are outright dissatisfied with one or more elements within their security stack.

While respondents pointed to a number of reasons for their dissatisfaction, the top two provide a double-whammy of a high rate of false positives and lack of efficacy. In other words, not only is the security product ineffective — a big enough problem on its own — but it also contributes to wasting the time and energy of already-burdened security personnel. On average, respondents reported that they or their teams spent over a day a week (9.4 hours) responding to false positives. Over the course of a year, this becomes 61.1 business days, or the equivalent of losing a team member for an entire quarter.

What are the causes of your dissatisfaction? *(select all that apply)*



TREND 2

Budgetary Pressures and Legacy Solutions Are Increasing Cyber Risk continued

Price is easy to measure, but is different from cost

Today's threat actors are simply too motivated, too persistent, and too well-equipped for organizations to place faith in the lowest-priced or most conveniently packaged security products.

A tendency to procure based mainly upon price simply hides the real cost of acquisition elsewhere — in wasted time, the associated opportunity cost, and the consequences of disruptive cyber attacks — and contributes to cybersecurity's effectiveness problem.

Instead, a cybersecurity product's capabilities, environmental fit, and support or service should be the most important evaluation criteria. Unfortunately, only 55% of respondents were able to say that their organization procured their current endpoint tooling based on "careful evaluation and best fit for our environment." That's barely half, despite many of those same organizations no doubt professing that cybersecurity is a priority.

55% **Only 55% of respondents were able to say that their organization procured their current endpoint tooling based on "careful evaluation and best fit for our environment."**

TREND 3

Organizations Are Managing AI Risk With Official Usage Policies

Security decision makers find themselves in the difficult position of evaluating the security risks of AI tools and services, and of developing policies on their adoption and usage.

For example, in addition to general concerns relating to hallucination and inadvertent plagiarism, there are very real privacy risks:

- Sensitive information — for example, proprietary data or personally identifiable information (PII) — entered into an AI utility could potentially be extracted by subsequent users (including those outside of the organization), constituting a data breach
- Data entered into these tools may be sent to third-parties in other countries, violating data sovereignty regulations or contractual agreements, and raising concerns about industrial espionage

There's every indication that organizations are taking a very mature approach to AI adoption and usage.

For one thing, fully 99% — up from 94% a year ago — of leaders surveyed indicated that their organization either already has an AI policy in place (86%) or plans to do so (13%). This leaves just 1% of organizations abdicating their responsibility to make an informed choice one way or the other.

And lest one assume that organizations are defaulting to a position of adoption, the survey shows that plenty of orgs are 'opting out,' so to speak. While roughly two thirds of respondents indicated that their company either already has a policy in place outlining proper use of these technologies (56%) or plans to implement such a policy (11%), that leaves nearly one third (excepting the 1% noted above) who have outright forbidden usage of LLMs and GenAI (30%) or who plan to do so (2%).

Does your organization currently have a policy in place in regards to best practices and acceptable use for the utilization and adoption of generative AI and Large Language Models? *(select one)*

TREND 3

Organizations Are Managing AI Risk With Official Usage Policies continued

Adopting a secure — and informed — position

The sudden arrival and widespread adoption of generative artificial intelligence (GenAI), in general, and LLMs in particular is perhaps without parallel.

Spurred by both a genuine interest in the revolutionary potential of these technologies and by a fear of falling behind competitors who wholeheartedly embrace them, organizations of all stripes are making tough choices.

It's heartening to see that fully 99% of organizations have already established, or will soon do so, a position with respect to the usage of AI within the workplace. The rapid implementation of corporate policies on the acceptable usage of artificial intelligence shows a possible turning point as decision makers are eager to break the cycle of playing "catch up" in securing technology adoption and instead prepare their organizations in advance.

To the 13% who plan to implement a usage policy one way or the other, we encourage you to do so sooner rather than later. And to the 1% who lack a policy and a plan, we'll politely suggest that it's better to be proactive on this issue, versus reacting after you're forced to by some unpleasant development.

Whether or not an organization has adopted a usage policy, security leaders would do well to monitor for AI utilities falling into the "shadow IT" category. Something as ubiquitous and promising as existing and emerging AI tools is very likely to find its way into an IT environment near you.

Finally, it's worth noting that a truly informed AI usage policy requires understanding regulatory and even contractual obligations, so leaders should be sure to work with their respective legal counsel to avoid surprises.

99% **99% of organizations have already established, or will soon do so, a position with respect to the usage of AI within the workplace.**

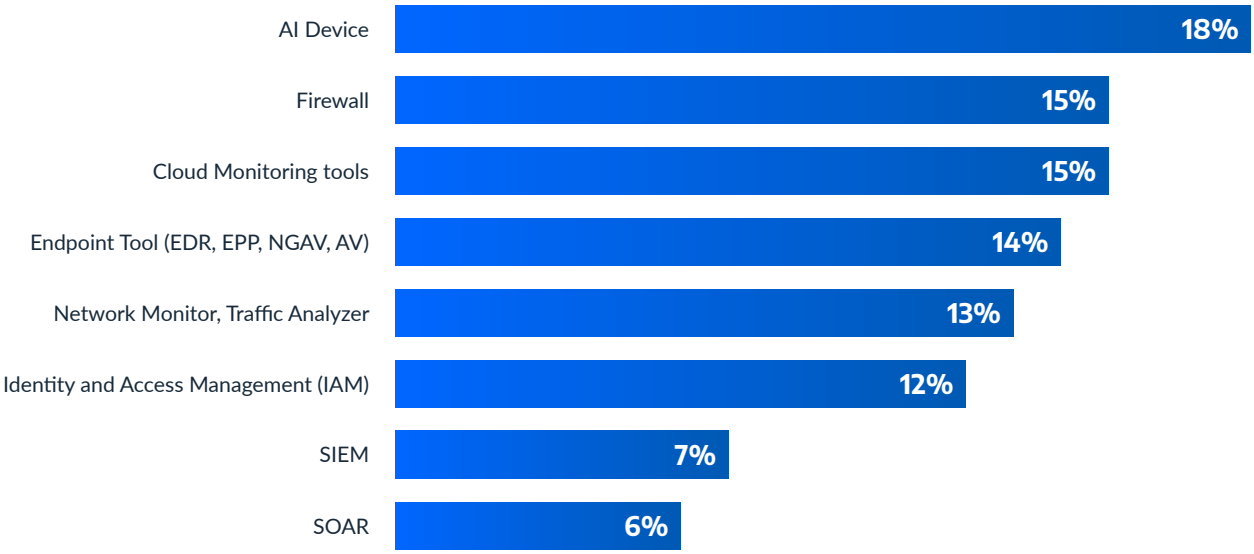
TREND 4

AI Devices Aren't Yet Ready For Prime Time

Due largely to the technology's ability to quickly analyze and — over time — learn from huge data sets, many security vendors have incorporated AI (particularly machine learning, or ML) into their solutions.

While the future may eventually be AI-driven, it certainly seems like there's considerable progress to be made before that's the case, as 18% of security leaders indicate that AI devices currently deliver the least amount of value — a higher percentage than for any other security device.

From which security device are you currently seeing the least value in your security program in terms of initial investment, time expenditure, and operating cost? *(select one)*



One reason for this comparatively lesser value is that AI devices still have an accuracy problem — nearly a quarter (24%) of respondents indicated that their AI appliances provided the highest amount of noise and false positives compared to true positive alerts, second only to network monitors and appliances (27%).

TREND 4

AI Devices Aren't Yet Ready For Prime Time continued

Getting from promise to practical may take a while

There's a difference between integrating AI into a proven solution compared to essentially making AI the solution itself.

In the former scenario, AI capabilities exist within and augment the broader set of people, processes, and technologies that combine to safeguard an organization; in the latter scenario — as is the case with AI devices being marketed today — entire security functions may be handed off to an AI engine.

Unfortunately, while AI devices are great during demonstrations, they tend to underperform in the real world. This discrepancy is at least somewhat due to impractically high false positive rates.

And even with today's technology, it remains much harder to improve an AI system's accuracy from 98% to 99.9% than it is to go from 85% to 90%. Crucially, though, that 1.9 percentage point increase reduces mistakes by a factor of 20, compared to only a one-third reduction for the 5 percentage point increase.

Accordingly, it will likely be a long time before the accuracy improves enough to put more trust in these devices. As historical context, it's taken roughly 25 years for credit card fraud detection to improve from about 80% accuracy in the late 1990s to today's extremely high level (approaching 99.9%).

For at least the next few years, the best cybersecurity outcomes will almost certainly use solutions that integrate AI to improve existing functions, versus handing the keys to AI devices.

It remains much harder to improve an AI system's accuracy from 98% to 99.9% than it is to go from 85% to 90%.

SECTION 3

Readiness Trends

TREND 1

Data Transformation and Secure AI Adoption Are Driving Heavy Cybersecurity Investments

A strong majority of respondents (84%) reported that their organization is investing heavily in its cybersecurity program, leaving only 16% admitting limited investments.

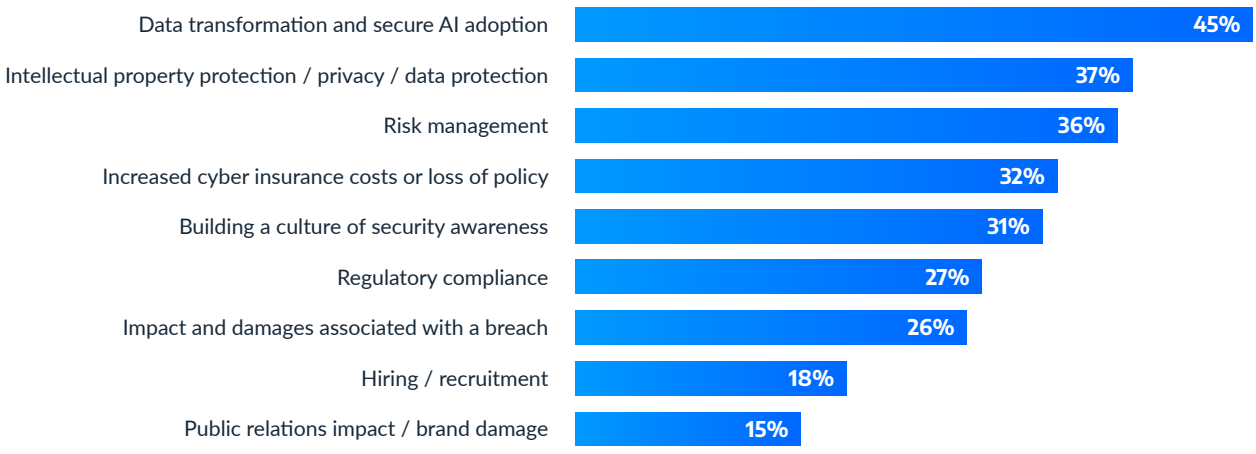
How would you classify your current cybersecurity investment?
(select one)

84% We invest heavily in our security program

16% We invest limitedly in our security program

Consistent with the earlier finding that AI is the primary area of concern for security leaders, the most frequently cited driver of cybersecurity investments was "data transformation and AI adoption," which was selected by 45% of survey respondents. In fact, there was a clear gap between the frontrunner and the next two major drivers, "intellectual property protection / privacy / data protection" (37%) and "risk management" (36%).

What do you feel are the primary drivers of your cybersecurity strategy for the next 12 months?
(select up to three)



TREND 1

Data Transformation and Secure AI Adoption Are Driving Heavy Cybersecurity Investments continued

At the risk of repeating ourselves...

The welcome news here is that, at least by their own standards, most organizations are investing heavily in cybersecurity.

The only point we'll make is that security leaders should do their utmost to ensure those investments are being directed in a prioritized manner, to maximize positive security outcomes.

For example, given the ubiquity and effectiveness of social engineering, training staff to recognize phishing lures, MFA bombs, and other common — and unfortunately effective — techniques is a cost-effective way to improve an organization's resilience. However, "building a culture of security awareness" was only selected by 31% of respondents.

Moreover, the **Arctic Wolf 2025 Threat Report** noted that "we see evidence that threat actors are adapting to target stronger cybersecurity postures by looking for novel methods of attack or embracing low-tech — but effective — means of bypassing high-tech safeguards." This observation underscores the point that most of cybersecurity is actually about addressing fairly mundane things like misconfigurations, patching vulnerable software, reducing Identity sprawl, implementing strong MFA, and so on.

So, while it's heartening to know that leaders are taking a responsible approach to AI and the technology's relationship to data, the hype around AI may distract from more important — and ultimately more effective — security investments.

31%

Training staff to recognize phishing lures, MFA bombs, and other common — and unfortunately effective — techniques is a cost-effective way to improve an organization's resilience.

However, "building a culture of security awareness" was only selected by 31% of respondents.

TREND 2

Most Organizations Are Satisfied With Their Cybersecurity ROI

When it comes to return on investment, the good news is that 71% of security leaders are satisfied with the value their organization is getting from its cybersecurity investments.

The bad news, though, is that 29% of respondents are dissatisfied.

Are you satisfied with the value you are getting from your cybersecurity investment? *(select one)*

71% Yes

29% No

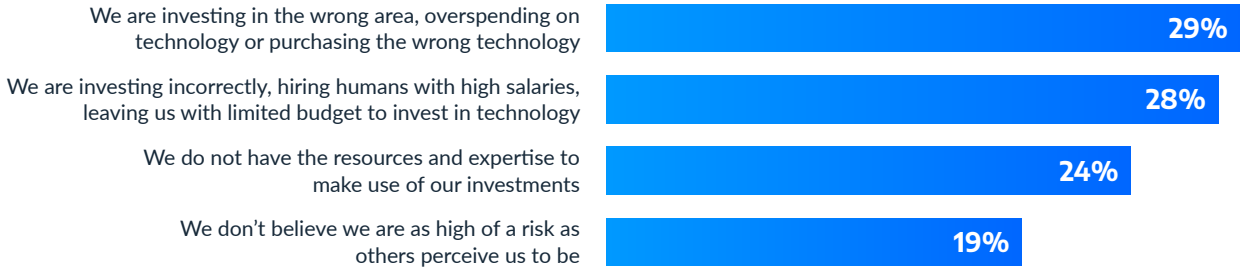
Of those dissatisfied respondents, 29% pointed to technology problems, indicating that their organization is either overspending on technology or buying the wrong technology.

Interestingly, a nearly identical proportion (28%) pointed to people problems, reporting that their organization pays so much in security salaries that they have insufficient funds for technology.

Just under a quarter of respondents (24%) noted that the culprit wasn't the investments themselves, but a lack of resources and expertise to get the most out of them.

Finally, 19% of security leaders pointed to a relative imbalance between their investments and the threats they face.

Why do you believe you are seeing limited return in your investment? *(select one)*



TREND 2

Most Organizations Are Satisfied With Their Cybersecurity ROI continued

Finding the balance that works for you

To address today's cybersecurity challenges, we believe organizations should take measures to assess, mitigate, and transfer their cyber risk.

A proven enabler of this ongoing journey is security operations (SecOps), which refers to the people, processes, and technology that all work together as a central hub to create and manage a security architecture for an organization. Whether delivered by an internal team, an external service provider, or a hybrid combination of both, benefits of a SecOps-oriented model include:

- Faster responses to threats and incidents, as measured by mean time to detect (MTTD) and similar metrics
- The stopping of potential threats before they become breaches
- More effective and efficient identity and access management
- Continually improved security posture
- A more unified approach to security

However, finding the right mix of people, processes, and technologies is a challenge. Likewise, selecting the right products and choosing what areas — if any — should be outsourced are also tough decisions.

The best advice we can offer is to make complementary invests in all three areas, equipping your organization with:

- Technologies that work with your IT environment (including your existing security stack)
- Skilled team members (whether in house or at a third party) who can get the most out of those technologies
- Processes that effectively and efficiently lead to your desired security and business outcomes

TREND 3

IR Retainers Become Ubiquitous and Are Getting Put to Use

Incident response (IR) is a set of processes and tools used to identify, contain, and remediate cyber attacks, and to restore the organization to pre-incident operations.

Important functions include:

- Securing an environment by eliminating the threat actor's access
- Analyzing the cause and extent of the threat actor's activities while inside the network
- Restoring the network to its pre-incident condition (including ransom negotiation and payment, if required)

Ideally, each function is performed concurrently and is complemented by information, insights, and outcomes emerging from the others.

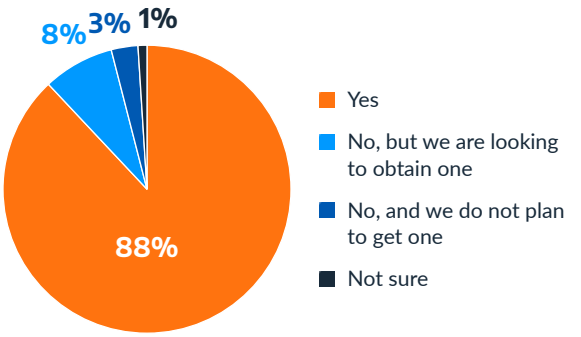
Vendors that offer IR services typically also offer IR retainers, and this model has been embraced by organizations seeking to transfer risk and ensure support during an incident.

Last year, we noted that "64% of organizations have currently invested in an incident response retainer, with another 26% planning to obtain one within the next 12 months."

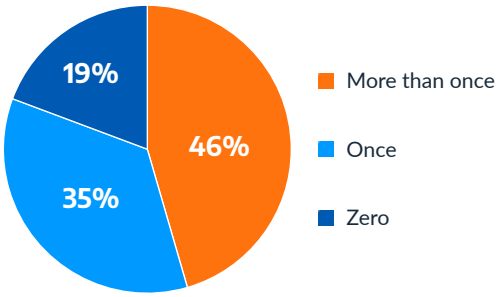
And it seems that respondents were telling the truth, as this year's survey revealed that 88% of organizations have purchased an active IR retainer, an increase of 24 percentage points. Plus, an additional 8% of security leaders noted that while their organization doesn't yet have an IR retainer, it is looking to obtain one.

Crucially, the importance of these retainers isn't just already proven — it's growing. Of those organizations with an IR retainer in place, 81% had to use it one or more times in the last 12 months (versus 70% last year). Perhaps even more telling, 46% activated it two or more times — a significant leap over last year's 30%.

Does your company currently maintain an incident response retainer or discretionary fund? *(select one)*



How many times has your company used its IR retainer or discretionary fund in the past year? *(select one)*



TREND 3

IR Retainers Become Ubiquitous and Are Getting Put to Use continued

Unsurprisingly, the most frequently cited reason — selected by 69% of respondents — for using the IR retainer or funds was in response to an incident. However, 29% indicated that they needed support for a non-incident related scenario.

Why did you utilize your IR retainer funds? *(select all that apply)*

Finding the right IR provider for your organization

The high rate of usage shows that modern IR retainers are more than a "nice to have" precaution and instead are a critical component of a modern security program.

However, it's important that leaders looking for an IR provider understand that there are two types of retainers: those with no up-front costs and those that are prepaid.

The no-cost IR retainer, also known as a zero-dollar retainer, is an excellent way to reduce the impact of cyber attacks by establishing a path to assistance, the terms of engagement, and a predetermined hourly rate ahead of needing to engage IR specialists. No-cost retainers may also provide preferred access to the IR team just like prepaid retainers.

Cyber insurance carriers will usually approve the use of reputable IR vendors that aren't included on their pre-approved list. To eliminate delays when IR services are needed, it's recommended that organizations obtain written confirmation of this from their insurance carrier once a retainer is established and before experiencing an incident.

IR costs are usually covered (less policy deductibles) by cyber insurance, but you'll want to review your specific policy and/or endorsements to determine how much coverage you may have.

Organizations that choose prepaid retainers are often looking for preferred access to IR teams or want to negotiate a lower hourly rate on a large block of hours.

Before purchasing a prepaid IR retainer, verify with your insurance carrier that the prepaid hours are covered by your cyber insurance policy. Spoiler alert: they probably are not.

TREND 4

Organizations Underestimate the Importance of Comprehensive (and Current) IR Plans

An incident response plan (IR plan) consists of documents, processes, and data sets that may be necessary to properly respond to a threat when one is identified.

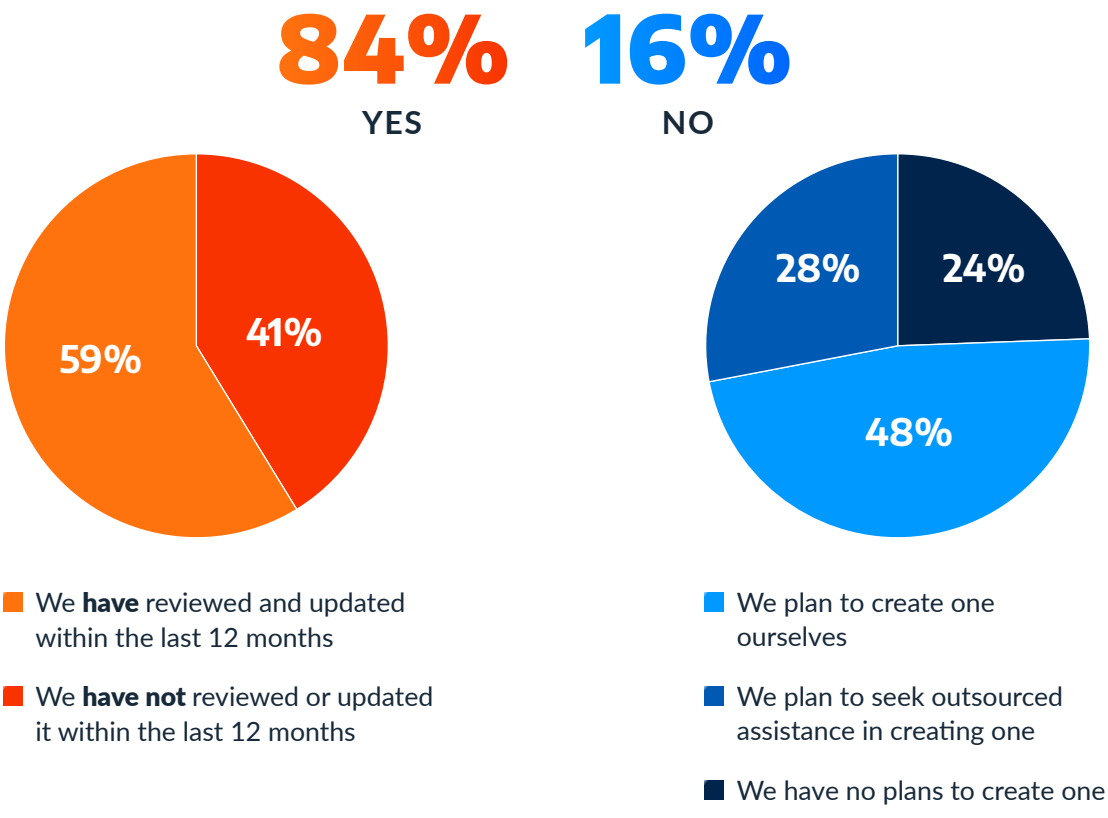
Additionally, many of these plans also include information about a third-party incident response retainer if one was purchased by the organization.

Yet, despite their importance, the survey revealed that only 60% of organizations have an IR plan in place, a decrease of four percentage points from last year.

Looking one layer deeper, only 59% of the organizations that do have a plan have reviewed and updated it in the last 12 months — a startling and worrying drop from last year's 83%.

Of the organizations that don't already have a plan, the encouraging news is that more than three quarters (76%) plan to create one at some point. Slightly less encouraging is that most of that group intends to craft the plan themselves, without any outside expertise.

Does your organization have an incident response plan? *(select one)*



TREND 4

Organizations Underestimate the Importance of Comprehensive (and Current) IR Plans continued

You know what they say about "Failing to plan..."

It should go without saying that an IR plan is an important element of an organization's overall preparedness.

After all, the IR plan is the roadmap during a crisis, providing details including contact lists (for both inside and outside the organization), designated decision makers and other areas of responsibility, and business continuity and disaster recovery plans.

Given its importance, the IR plan should also be updated in response to changing IT environments and operating contexts. Moreover, even without significant changes, the IR plan should be regularly reviewed — at minimum every six months — to ensure efficient and effective execution at a moment's notice, perhaps during a true crisis.

Why, then, do only 35% of organizations have an up-to-date IR plan?

Without deeper conversations with the respondents, it's impossible to say for sure.

However, here are two plausible explanations.

01

First, in many organizations, cybersecurity has a technology bias. That is, it's regarded as predominantly providing technology solutions to technology problems. In such a context, things like processes, workflows, and plans take a backseat.

02

Second, it's reasonable to wonder if the widespread adoption of IR retainers may be causing some security leaders to presume they can outsource all aspects of incident response, obviating the need to have an internal IR plan. This is a dangerous belief, as a truly effective incident response capability goes beyond merely having an IR retainer. Rather, it's crucial to have a strong IR plan that covers not only the technical aspects of IR but also business continuity, roles and responsibilities, and other aspects.

35% **Only 35% of organizations have an up-to-date IR plan.**

Conclusion

As the security leaders who participated in our survey know all too well, cybersecurity continues to evolve at a rapid pace:

New threats, risks, and associated concerns continue to appear

Mitigation strategies that worked in the past become less effective, creating a need for new approaches — some of which might not yet be ready for prime time

Preparedness — including risk transfer strategies — remains vital, and often means the difference between an unpleasant blip and a breach with long-lasting repercussions

At the center of rapid change is AI, causing security leaders to grapple with how to better secure their organizations from AI-enabled attacks as well as how they will address the potential threats and vulnerabilities that come with the proliferation of AI tools and applications across the enterprise.

Notably, at this current juncture, AI has become both a primary source of concern for security teams while also being heralded as the solution as more and more AI-powered security offerings come to market.

AI will continue to reshape the cybersecurity landscape, but the challenge here is not reinventing cybersecurity, it is evolving and adapting by reinforcing and extending existing security frameworks and controls, enabling security teams to manage AI-driven risks without overhauling their entire security infrastructure.

We hope that this report has shown you that you're not alone — both in experiencing the stresses of being a security leader and in the ongoing battle against those with malicious intent.

But our larger hope is that the results of this survey and the accompanying analysis and commentary will help you, your team, and your security vendors to work together to build a stronger security posture for the rest of 2025 and beyond.

How Arctic Wolf Can Help

As a market leader in security operations, Arctic Wolf can help close the gaps in your cybersecurity defenses, manage your risks, and deliver comprehensive incident response services to address escalated threats.

The Arctic Wolf Aurora™ Platform delivers automated threat detection and response at scale and empowers organizations of virtually any size to stand up world-class security operations with the push of a button.

END CYBER RISK

ARCTIC WOLF

About Arctic Wolf

Arctic Wolf® is a global leader in security operations, enabling customers to manage their cyber risk via a premier cloud-native security operations platform.

The Arctic Wolf Aurora™ Platform ingests and analyzes more than eight trillion security events a week to help enable cyber defense at an unprecedented capacity and scale, empowering customers of virtually any size across a wide range of industries to feel confident in their security posture, readiness, and long-term resilience. By delivering automated threat protection, response, and remediation capabilities, Arctic Wolf delivers world-class security operations with the push of a button.

For more information about Arctic Wolf, visit **arcticwolf.com**.

REQUEST A DEMO