ARCTIC WOLF

THE STATE OF CYBERSECURITY

2023 TRENDS

Table of Contents

01 Foreword

01 Foreword

As 2022 came to a close, we found ourselves nearly three years removed from the start of a global pandemic that forced IT and security teams to take on the herculean task of shifting organizations to entirely remote work models overnight.

While some of the initial security challenges posed during the height of the pandemic have been solved for and can be viewed from a comfortable distance through the rearview mirror, there are challenges that either arose or intensified during this disruptive period that remain issues for security teams today.

The 2023 Arctic Wolf State of Cybersecurity Trends Report took the temperature of organizations around the globe and sought to understand not only their current and future concerns, but how they were responding to the problems that had plagued them in previous years. Our research shows that, despite the enduring nature of many of these challenges, organizations are making measurable strides in areas where progress has proven limited in previous years.

In the era of the dispersed workforce, organizations are doubling down on end-user security, and with it, a culture of security awareness has gained traction. Cloud security, a perennial issue that is a mainstay of "top challenges" lists is a principal area of investment and focus of continued learning for organizations, showing that 2023 may be the year where real headway is made in advancing cloud security outcomes. Risk management was recognized as the most urgent concern driving security strategy, indicating a momentous shift in thinking around the value of proactive security.

But among these bright spots, perennial security challenges remained. Ransomware grew in volume and impact — and organizations were, unfortunately, willing to pay — while the number of organizations who found themselves breached reached new, startling levels. Patch management continues to be a struggle for organizations, even as long-lived vulnerabilities become an increasingly exploited attack vector.

Additionally, a lack of cybersecurity expertise remains a recurring challenge for organizations.

Rather than addressing isolated concerns, in 2023 organizations must adopt a security operations mindset that informs cybersecurity decisions across the full range of operations.

Organizations that can rely on a mature security operations practice will find themselves more secure, more resilient, and better able to adapt to the multitude of internal and external risk factors.

Methodology

The survey was conducted among 701 IT directors and above working in companies with more than 50 employees, from the USA, UK, Canada, South Africa, DACH (Germany, Austria, Switzerland), ANZ (Australia, New Zealand), and the Nordic regions (Norway, Sweden, Denmark, Finland) during December 2022.

At an overall level, results are accurate to ± 3.7% at 95% confidence limits assuming a result of 50%.

02

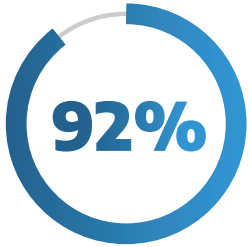
2023 Areas of Investment: Cloud Security and Security Awareness Training

02 2023 Areas of Investment: Cloud Security and Security Awareness Training

As we enter a new year, the leading area of investment for organizations is in securing their cloud resources.

Of those surveyed, 53% stated that they currently have plans to add or update their cloud security technology within the upcoming calendar year – a 31% increase from what respondents reported a year prior.

This is a positive trend that matches security gaps many organizations are facing within their infrastructures.



Arctic Wolf's threat detection data for 2022 showed that over 47% of threats we respond to include a compromised cloud component, and 92% of organizations have an active cloud security gap within their infrastructure.

The second leading area of investment for 2023 is in the implementation of a security awareness program.

40% of our respondents stated that they are actively planning to implement a security awareness program within their organization within the coming year. This is an excellent plan when we consider that over 90% of the threats Arctic Wolf responded to in 2022 actively targeted employees or users. In many cases, social engineering or phishing is the easiest method for attackers to obtain credentials and initial access.

Security awareness programs help users understand how these threats play out and how they themselves are often both the target and the first line of defense.

It's a proactive step that can stop an attack in its tracks. If you combine a high-quality awareness program with active monitoring technology for indicators of a successful phishing attempt, you're setting your organization up for success. This combination prevents a strong security technology stack from being defeated by a complacent user giving away credentials to a crafty social engineer.

03

Ignoring a Major Risk Management Investment

03 Ignoring a Major Risk Management Investment

A major solution being left out of organizations' plans is patch management.

18%

Only 18% of survey respondents plan to implement or improve their patch management system within the next year.

Exploited vulnerabilities are a growing issue, and research from the Ponemon Institute on vulnerability response states that 60% of breaches could have been prevented with a proper patch.

While patching every vulnerability that pops up is an unrealistic solution, ignoring your patch management system, or not investing in vulnerability management, will only increase risk.

In fact, the 2023 Arctic Wolf Labs report found that four of the top five external software exploits utilized by threat actors in 2022 were published in 2021.

04 Searching For Value: Endpoint Technology Is Critical, but Not the Only Solution

04 Searching For Value: Endpoint Technology Is Critical, but Not the Only Solution

Just as organizations are prioritizing what could offer the most value to their security environment, they are also evaluating which solutions are providing the least value.

30%

One data point came as a surprise — 30% of organizations stated that their current endpoint technology tool provides the least value.

This dissatisfaction in endpoint technology likely comes from a few issues:

- Some organizations may be using an endpoint technology that is the wrong fit for their organization. Although there are a wide range of valuable endpoint tools on the market, they are not all equal in their capabilities. In some situations, a business may have bought into a tool that just wasn't right for their needs.
- Many endpoint tools are powerful, but it must not be forgotten that they are often simply that — tools. Without the proper team of analysts to actively monitor, manage, and respond to these tools on a continual basis, an organization may be stuck with a product triggering a series of alerts that no one is available to respond to. What good is a fire alarm if no one is there to hear it?
- The market may be coming to a crucial realization: While endpoint tools are an essential component of security visibility, they are only a piece of the puzzle that allows security teams to identify and respond to threats effectively.

All these issues point to a shift toward technology that offers more than just EDR.

04

Searching For Value: Endpoint Technology Is Critical, but Not the Only Solution

Two EDR-adjacent options: managed detection and response (MDR) and network traffic analysis (NTA), received much lower dissatisfaction rates from respondents, at 14% and 13%, respectively.

The inverse of this data reveals that organizations are finding the most value in these EDR alternatives.

NTA allows security teams to detect threats at the network level.

It is true that almost any breach will inevitably reach an endpoint, hence the value of endpoint visibility and endpoint security technology. However, pairing network traffic analysis with an endpoint technology allows for higher fidelity alerting and faster detection time. Quite often threats can be detected within network telemetry and then validated once they have reached the endpoint.

As for managed detection and response, this answers the question of who will utilize the tools that the organization has invested in.

A quality MDR provider should be able to build upon and supplement an environment's existing security stack by monitoring and responding 24x7. With this definition of MDR, it's easy to see how many organizations find immediate value in this service.

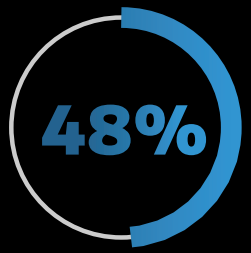
05

2023's Top Concern: Ransomware Returns, and It's Only Growing

05

2023's Top Concern: Ransomware Returns, and It's Only Growing

One word appeared over and over when it came to organizations' biggest concerns in 2023: ransomware.

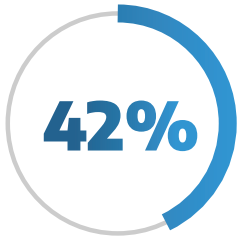


48% of organizations rank ransomware and targeted threats as their number one concern for the upcoming year.

This was also the top concern in the 2022 version of this report, and for good reason.

Ransomware attacks continue to grow, and the growing popularity of ransomware-as-a-service (RaaS) has lowered the barrier for novice attackers to execute this style of attack.

We believe that this trend will only continue for the foreseeable future. That is why it is so important for organizations to continually identify their security gaps, actively train their users in security awareness, and develop a strong response plan in the event they are subject to a ransomware attack. Ransomware concerns are backed up by continued attacks.



42% of organizations surveyed suffered a ransomware attack in 2022, with an additional 3% claiming to be unsure if they were victims.

This leaves only 55% of environments unaffected by a ransomware attack in the previous 12 months. Those respondents who felt unsure could be the result of identifying and preventing a potential ransomware attack before it reached the payload deployment or detonation stage.

05

2023's Top Concern: Ransomware Returns, and It's Only Growing

Not only are organizations getting hit with ransomware attacks, but they may be inspiring future attacks by paying the demanded ransom.

74% of the time someone, either the victim themselves or a representing body, such as an insurance company, chose to pay some percentage of the ransom.

Once results were broken down further, an interesting balance in the way those affected chose to respond was revealed.

26% took the hardline approach of not paying any of the ransom demand. Another **11% chose not to pay themselves** but allowed an insurance provider or outside entity to pay some portion of the ransom. In **41% of the cases, the victims chose to pay the ransom in full**, while the remaining **22% agreed to only pay a portion of the ransom** that was negotiated with the attackers.

It's worth noting that many law enforcement agencies, including the FBI, take the position of never paying the ransom as this only emboldens attackers. Unfortunately, we understand that every situation is unique and, while refusing to pay may seem morally correct, it may not be the best option for many victims.

06

Additional Concerns for 2023: Cloud Security, Vulnerabilities, and Data Confidentiality

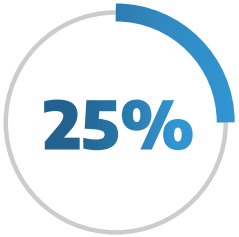
06 Additional Concerns for 2023: Cloud Security, Vulnerabilities, and Data Confidentiality

The second-most common concern identified was in the area of cloud security gaps, with 42% of respondents stating that this was their primary area of worry.

This trend directly correlates to the previously identified top area of investment in 2023 being cloud security.

When asked about the current state of their cloud security posture, only 38% of respondents believe they are effectively securing their cloud resources.

The remaining results indicate that many organizations see cloud security as a "best effort" area, with 26% also claiming cloud is one of their biggest security weaknesses.



Interestingly, 25% of our respondents noted that vulnerabilities and patching was their biggest concern in 2023.

While there is great value in focusing on remediating vulnerabilities, this statement runs contradictory to where many organizations seemingly plan to invest in the upcoming year. It's difficult to identify exactly why this is, but it may lie in reduced security budgets and prioritizing what they feel are the largest areas of concern.

07

Organizations Want to Understand Cloud Threats Better

07 Organizations Want to Understand Cloud Threats Better

As organizations develop their budgets and plans for the upcoming year it's important that they identify their largest areas of concern and what they see as their biggest security gaps.

It's also important for these organizations to identify areas where they would like to learn more.

Cybersecurity is an ever-evolving landscape and leaders in this space must pay special attention to ensuring they stay current with evolving threats and emerging technologies.

Respondents selected cloud security and evolving infrastructures as the area of cybersecurity they would like to learn more about in the coming year.

This area is important for organizations to understand and stay current on. The further adoption of work-from-home architectures and distributed, digital environments have eroded the traditional network perimeter. Couple this with the financial incentives of cloud adoption and it's easy to see why the cloud is becoming a growing area in information technology. As these vulnerable environments continue to grow and evolve, so must the security teams tasked with monitoring and protecting these architectures.

Beyond their learning interests, survey participants were asked what they saw as their primary objective for the upcoming year — reducing costs, increasing response time, and achieving or maintaining compliance were all options.

However, data confidentiality topped the list, with 45% of responses.

Many organizations see this as their goal to prevent breaches and stop data leaks. This makes sense when we consider data loss and data leaks can often lead to further security concerns. For example, credential leaks could serve as an initial access point for more sophisticated compromises or ransomware attacks.

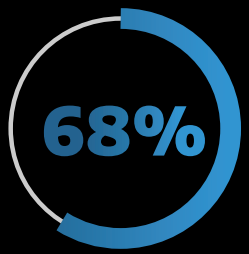
Lack of data confidentiality can also result in loss of personally identifiable information (PII), trade secrets, and confidential company information, all of which could result in monetary or reputational damage.

08

Top Barrier: Staffing Is Keeping Organizations from Achieving Their Objectives

08 Top Barrier: Staffing Is Keeping Organizations from Achieving Their Objectives

So, what is stopping organizations from reaching the above objectives? Just as it was last year, the top answer for 2023 is staffing.



Aligned with the results from our 2022 report, 68% of organizations identified staffing related issues as the number one threat to achieving their objectives.

This is broken down into 32% of organizations having difficulty with hiring and retaining staff, and 36% of organizations who feel their current staff lacks the necessary expertise needed for their goals.

This year's survey provides more insight into just how many bodies are needed to fill this gap.

56% of respondents believed they would need to hire **five** or more full-time staff members, while 48% have increased that to **10** or more full-time dedicated cybersecurity members. 8% of our respondents believe they do not need to currently hire anymore staff members and they feel as though they are fully staffed. This shows that a minority of organizations feel their cybersecurity teams are fully staffed.

The security skills gap has been a known problem for some time and to overcome this some organizations have turned to hiring under-skilled workers to fill much-needed positions.

08

Top Barrier: Staffing Is Keeping Organizations from Achieving Their Objectives

It is admirable to hire under-skilled analysts to provide them with the ability to learn and enhance their skill sets.

Unfortunately, this practice commonly occurs in organizations that are short staffed, and in desperate need of analysts. As a result, these under-skilled staff members are placed in positions they may not be qualified for and that don't provide the proper time to learn.

Organizations that follow this path are potentially setting themselves and their analysts up for failure resulting from missed alerts, misunderstanding of detections, and the inability to deal with alert fatigue.

Hiring more novice analysts is an important part of developing a security team, but only if training and skill development are foundational within their job function.

Interestingly, the remaining challenges listed represent an even distribution across all the organizations surveyed.

This includes lack of cybersecurity budget, lack of visibility into emerging threats, lack of awareness/ support from leadership, future economic uncertainties, and competing technology priorities.

While only 5% stated they do not see any challenges, all organizations should be prepared for potential threats.

Threats are a matter of if, not when, so we hope that these 5% of organizations are not setting unrealistic expectations and are fully prepared for any potential challenges that may arise.

09

Risk Management Drives Organizations' Security Decisions

09 Risk Management Drives Organizations' Security Decisions

Identifying what drives your cybersecurity program helps focus where you should budget and how to prepare for your organization's security future.

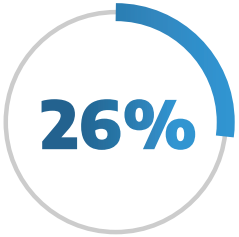
When asked about the most urgent concerns driving their organization's cybersecurity strategy, respondents shared risk management as a top theme along with recruiting and retaining security staff.

30%

30% of respondents reported risk management as the top concern driving their organization's cybersecurity strategy.

The frequency and ease at which threat actors have been able to exploit vulnerabilities across IT environments has at least in part given organizations the push needed to move from recognizing the value of risk management in theory, to realizing its value in practice.

In pursuit of increased resilience, organizations supplemented existing threat-driven reactive measures with repeatable, proactive risk management processes.



26% of respondents reported increased cyber insurance costs/ loss of policy as a driver of their cybersecurity strategy.

Organizations are becoming more interested in obtaining cyber insurance as a means to transfer risk, especially risk associated with ransomware attacks.

The Arctic Wolf State of Cyber Insurance Report, which explores how global IT executives are addressing challenges and changes in the cyber insurance market, showed that the highest-ranking motivation to obtain cyber insurance globally was that it is a risk management best practice.

21% of organizations stated their primary driver is recruiting security staff. A common concern felt throughout the market is that organizations have overinvested in technology and now lack the necessary skilled analysts to utilize those tools. As mentioned above, the skills gap can cause major issues within an organization's security architecture.

10

Bigger Bucks: Security Budgets Continue to Grow as Threats Evolve

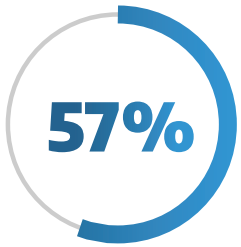
10 Bigger Bucks: Security Budgets Continue to Grow as Threats Evolve

Budgeting for a cybersecurity program can be a difficult task.

In addition to the costs related to tools and technology, a security manager must also consider discretionary budgets for salaries (both current and future), training and development, insurance, and the costs associated with potential compliance fines and fees.

Compounding this figure are the unexpected costs the security team fears the most, including ransomware payments or the expenses associated with recovering from an incident.

Therefore, it's easy to understand why so many organizations expect their cybersecurity budget to increase in 2023.



57% of organizations are planning to increase their cybersecurity budgets in 2023.

A small portion of those — 15% — are expecting a dramatic increase. Last year only 7% were planning a dramatic increase, so big moves are being made across businesses.

It is also worth noting that, of the 43% that do not believe their budget will increase this year, many believe their stagnant budget has little to do with their cyber preparedness. Instead, we found through discussions with individuals tasked with budgeting that many organizations are locked into situations where an increase is simply not possible. This could be due to lack of available funds, or not receiving leadership approval for any form of budgetary increase.

In many cases this may turn out to only be a temporary cost-saving measure. Unfortunately, many of these companies may find themselves in a difficult situation where additional funds must be obtained due to unforeseen circumstances, such as a data breach. Considering that a breach is often a matter of when, not if, these organizations are putting themselves in a reactive cycle, where more time and funds will be spent reacting to threats instead of proactively reducing the risk of future threats.

11 To Disclose or Not To Disclose? How Organizations React After a Breach

11 To Disclose or Not To Disclose? How Organizations React After a Breach

Many factors are involved in the likelihood of an environment suffering a breach, but everyone is at some level of risk when it comes to being a victim.

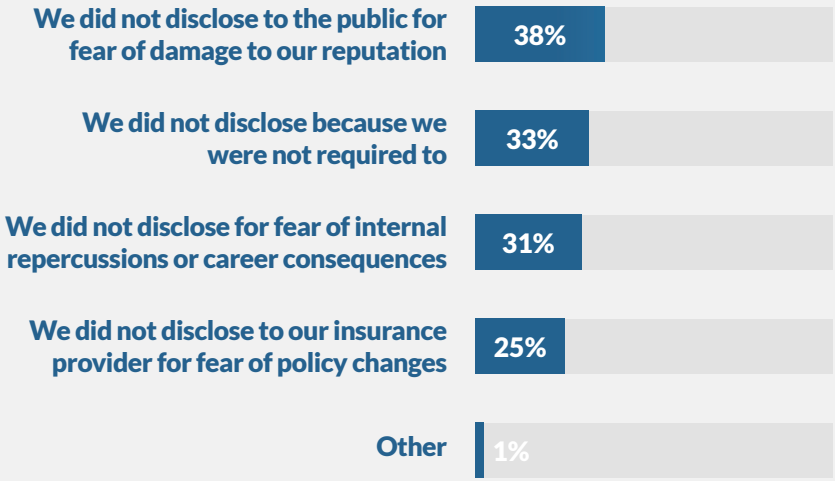
50%

50% of organizations admitted to suffering a breach within the last year. That places the chances of being the victim of a compromise right alongside the flip of a coin.

72%

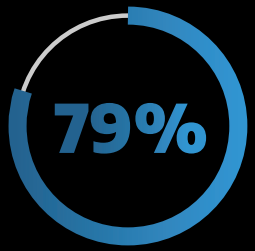
Of the respondents that admitted to suffering a breach, 72% of them chose not to disclose this information, while only 28% did make some aspect of their breach known.

Which of the following options are reasons you didn't disclose the breach?



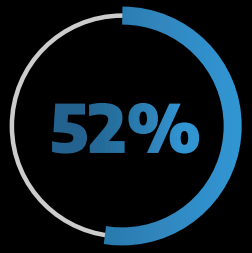
Despite the reasoning, we have yet to enter a phase of cyber defense where breaches can be openly disclosed and discussed without some level of concern.

11 To Disclose or Not To Disclose? How Organizations React After a Breach



Of the organizations that suffered a breach but did not disclose it, 79% reported having either an incident response (IR) retainer or incident response discretionary fund.

While the necessary information isn't available to determine what role, if any, an IR retainer or funds played in the decision to keep breaches concealed, by design, IR retainers and discretionary funds reduce costly downtime or cover costs associated with a breach – potentially reducing reliance on cyber insurance to cover the cost of claims and diminishing the need to report.



Interestingly, 52% of the organizations who reported maintaining IR retainers or IR discretionary funds have not experienced a breach.

This is consistent with trends showing that thinking around the likelihood of suffering a security breach is reaching a tipping point, where organizations see the value in proactively preparing for their response to and recovery from a breach.

How Arctic Wolf®
Can Help

As this report reveals, cybersecurity continues to evolve at a rapid pace.

In a time of new sophisticated technologies, emerging threats, and a growing attack landscape, it's never been more important to ensure your organization's security. Keep the results of this survey in mind as you work with your team to build a stronger security posture for the rest of 2023 and beyond.

Arctic Wolf is a market leader in security operations, so we can help close the gaps in your cybersecurity defenses, manage your risks, and provide customized compliance reporting.

The Arctic Wolf® 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.

For more information about Arctic Wolf, visit arcticwolf.com