ARCTIC WOLF

2024

THE STATE OF CYBERSECURITY: 2024 TRENDS REPORT

Table of Contents

Foreword

In the past year, IT and security leaders faced off with digital sprawl and the profound impact of emerging technologies like generative AI. The growth of attack surfaces has left organizations with more potential exposures from vulnerabilities and misconfigurations rife for exploitation in the evolving threat environment.

The Arctic Wolf State of Cybersecurity: 2024 Trends Report took the temperature of organizations around the globe and sought to understand how they were responding to these areas of challenge.

Our research revealed that ransomware continues to be a perennial area of concern. For the third year in a row, ransomware ranked as the top concern for respondents. This concern is not without merit when we consider that 45% of the organizations we spoke with admitted to being the victim of a ransomware attack within the last 12 months, a 3% increase over last year.

Business email compromise (BEC) emerged as a top attack method with 70% of organizations sharing that they were targets of an attempted BEC attack within the last year. Additionally, our data showed most organizations surveyed identified an insider threat within the past 12 months.

Our research also revealed that in the face of growing attacks, IT and security leaders are prioritizing cyber resilience by increasingly implementing risk mitigation and risk transfer activities. Organizations are actively preparing to respond to incidents, with nearly two-thirds of organizations surveyed having a formalized incident response (IR) plan or incident response discretionary fund as part of their security program. And, an incredible 95% of organizations report either currently having or are in the process of obtaining a cyber insurance policy in the next 12 months.

While the growing adoption of specific risk mitigation and transference activities is encouraging, the path to true cyber resilience begins when organizations can establish a cyber risk baseline and measure its progress. From there, organizations are able to mitigate risk by understanding their cyber security posture and maturity and how that correlates to resourcing decisions, business risk mitigation and resilience strategies, cyber insurability, and much more.

If you're looking for a partner to help address end-to-end cyber risk at your organization, we encourage you to experience The Arctic Wolf Security Journey.

Throughout your Journey, Arctic Wolf works with you to holistically address cyber risk by equipping you with the tools and expertise to assess, mitigate, and transfer your cyber risk – and drive security outcomes.

Methodology

The survey was conducted among 1,000 IT and security decision makers at director level or above 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, from organizations with 50+ employees during March 2024.

In this particular study, the chances are 95 in 100 that a survey result does not vary, plus or minus, by more than 3.1 percentage points from the result that would be obtained if interviews had been conducted with all persons in the universe represented by the sample.

01

SECTION ONE: THREAT TRENDS

Data Breaches Continue at Alarming Rate

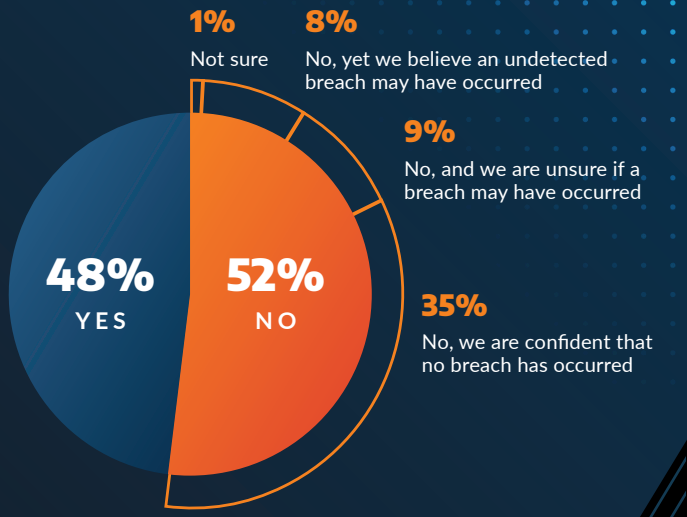
01

SECTION ONE: THREAT TRENDS

Data Breaches Continue at Alarming Rate

The threat of cyber attacks has long been a major business concern for organizations of all sizes and across all verticals, and this concern is not without merit.

Our research found that, within the last 12 months, 48% of organizations identified evidence of a successful breach within their environment. To fully understand the gravity of this statistic, it is important to understand that, although 48% of these environments found evidence of a data breach, that does not inversely mean that 52% of organizations did not suffer a breach.



Instead, it should be more accurately stated that the remaining 52% did not identify indicators of a breach within their environment.

This could be the result of multiple factors beyond a breach simply not occurring, from lacking the needed technology to identify indicators of a breach, misconfiguration of their security tools, lacking the expertise to recognize evidence of a breach, or a combination of these factors.

As we looked deeper into our results, we found that only 35% of the respondents who did not identify a breach within the past 12 months expressed confidence in their determination that a breach had not occurred, while another 17% of respondents admitted they were unsure if a breach had occurred. Within this "unsure" group, 8% expressed a high rate of confidence that a breach had occurred within their environment but went undetected by their existing security tools.

01

SECTION ONE: THREAT TRENDS

Data Breaches Continue at Alarming Rate

Of the organizations that admitted to positively identifying a breach within the last 12 months, our results found that 66% chose to publicly disclose information regarding their breach.

Another 30% of those breached chose to be more limited in their disclosure, only disclosing information regarding the breach to those who were impacted or those parties they were obligated to disclose information to. This left only 4% of breached organizations choosing to not disclose information about the incident at all.

These results show that, in total, 96% of those breached disclosed some aspect of the incident.

This is a vast increase over 2023 where only 26% of those breached chose to disclose any or all of the information regarding their incident.

This increase may be contributed to numerous factors, including the continued adoption of cyber insurance and the need to disclose incident information when filing a claim, the decrease in stigma that a breach is a "failure" of a security program, the adoption of state and federal laws regarding proper disclosure such as the expanded FCC data breach notification rules, and others. This drastic increase in breach disclosure can be seen as a positive trend, since it notifies more parties who may be negatively impacted by a breach.

02

SECTION ONE: THREAT TRENDS

Business Email Compromise Still a Top Method of Attack

SECTION ONE: THREAT TRENDS

02 Business Email Compromise Still a Top Method of Attack

After determining that almost half of our respondents identified a breach within their environment within the past 12 months, along with an undetermined number of additional victims who were unable to identify indicators of a breach, we wanted to learn more about the details of what occurred during some of these incidents.

Business email compromise (BEC), or email account takeover (EAT) attacks are on the rise across industries, as noted in the Arctic Wolf Labs 2024 Threat Report, which showed BEC attacks made up 29.7% of Arctic Wolf Incident Response engagements in 2023.

70%

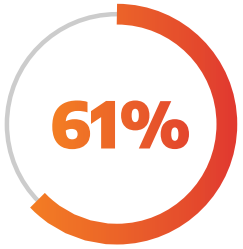
This survey found that 70% of organizations were the targets of attempted BEC attacks within the last year.

Within this group of targeted environments, 21% were able to prevent the attempt(s), 20% suffered at least one successful BEC event as part of a larger compromise, and 29% were the victims of one or more successful isolated BEC occurrences. The remaining 30% of environments fall into the category of either not being the target of BEC attacks or being unable to determine if one occurred.

With many organizations moving to cloud-based email services like Office365, these types of attacks can be difficult to identify with traditional security tools and may go undetected until they have successfully executed their objectives. This is why it is important when adopting O365 or alternatives to employ detection tools or services specifically designed to monitor for threats related to BEC.

02 Business Email Compromise Still a Top Method of Attack

Another threat that can have a devastating impact on an organization is one rooted in a malicious, negligent, or accidental insider threat incident.



Our data shows that 61% of organizations identified an insider threat within the past year.

This further breaks down into 29% of environments where the insider threat resulted in a security incident being declared, while 32% of the time the insider threat was identified, and the situation resolved before it escalated to the level of a declared security incident.

Additionally, of the 39% of those who did not identify an insider threat within the last year, 6% acknowledged that they believe they are at high risk of an insider threat occurring.

Not all insider threats are malicious in nature.

In some cases, an insider threat can be an uneducated user who executes an action that could result in a security incident, such as downloading potential malware, clicking on phishing links, leaving their laptop unattended in a public space, and more.

These types of insider threats can often be deterred when an organization makes use of a successful security awareness program.

03

SECTION ONE: THREAT TRENDS

Ransomware Remains Top Concern

03

SECTION ONE: THREAT TRENDS

Ransomware Remains Top Concern

In our annual research, we ask organizations what their primary area of concern is regarding cybersecurity, and for the third year running ransomware ranked as number one, with 51% of respondents citing it as their top concern — a slight increase from 2023's 48%.

45% of the organizations we spoke with admitted to being the victim of a ransomware attack within the last 12 months

91% of reported ransomware events included a data exfiltration component

This concern is not without merit when we consider that 45% of the organizations we spoke with admitted to being the victim of a ransomware attack within the last 12 months, a 3% increase over last year. An additional 2% acknowledged being unsure if they were the victims of a ransomware attack. This is likely due to a threat being detected and neutralized before the infiltration and detonation of the potential ransomware package.

Our results highlight the evolution of ransomware beyond the traditional approach of simple data encryption into what is often now a multifaceted attack that can include data exfiltration and potential extortion. Our results show 86% of ransomware attacks included successful data exfiltration with another 5% of security teams successful in preventing the attempt of data exfiltration during the attack.

This results in 91% of ransomware events including a data exfiltration component beyond the data encryption aspect of the attack.

03 Ransomware Remains Top Concern

Interestingly, only 57% of victims were notified of the data exfiltration by the ransomware perpetrators.

In their communications, these threat actors included data release prevention as part of the ransom demand.

The remaining 29% of victims who identified successful data exfiltration as part of their investigation into the event were not notified by the perpetrators.

In these circumstances the threat actors would likely have been planning a secondary extortion attempt threatening the unauthorized release or other malicious usage of this stolen data.

Statistically every ransomware victim environment employed some form of endpoint security technology, whether it be an endpoint prevention platform (EPP), endpoint detection and response (EDR) tool, a next generation antivirus (NGAV) solution, or combination thereof.

Inversely, we found that, of those environments that fell victim to a successful ransomware attack...

62%

62% were **NOT** utilizing a SIEM or SIEM-alternative for event log analysis, and

67%

67% were **NOT** employing network traffic analysis (NTA) to monitor for threats at the network level.

If we were to look at this data from another perspective, organizations that included analysis of network traffic and active monitoring of event logs for threat detection were less likely to be the victims of a successful ransomware attack.

04

SECTION ONE: THREAT TRENDS

Ransomware Attacks Leave Increasingly Steep Financial and Productivity Impacts

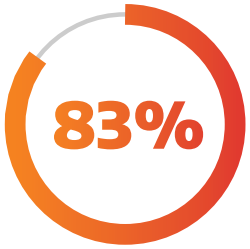
04 Ransomware Attacks Leave Increasingly Steep Financial and Productivity Impacts

We have collectively learned that ransomware can have devastating results on an organization's productivity. In our research, we sought to further understand and quantify this impact in greater detail.

In the Arctic Wolf Labs 2024 Threat Report, our Arctic Wolf Labs team found the current median ransom demand to be $600,000 USD.

$600K Current median ransom demand

> **This figure is important to note when combined with our latest research that also found victim organizations paid either some or all of the ransom demand 83% of the time.**



Victim organizations paid either some or all of the ransom demanded 83% of the time.

This was a significant increase from the 74% payment rate we identified in 2023 and shows that, with the amount of each payment and the percentage of times they are successfully being paid, these threat actors have no incentive to minimize their number of attacks.

04 Ransomware Attacks Leave Increasingly Steep Financial and Productivity Impacts

At Arctic Wolf, our position aligns with the general recommendations of the FBI: If possible, ransom demands should not be paid, as this is the only way we can hope to discourage these attacks. However, the decision on whether to pay is one that must be made by stakeholders within the victim organization once presented with all possible evidence and options.

If a victim chooses to pay the ransom demand, Arctic Wolf recommends employing the services of a professional ransomware negotiator. Among other benefits, these professionals can first help determine if the threat actor is a terrorist organization or sanctioned entity, in which case payments to them could be categorized as a criminal offense.

The financial impact of a ransomware attack also goes beyond the cost of the ransom demand alone, as these events often result in prolonged network and business downtime.

94% of those who suffered a ransom event experienced a period of significant downtime and delays in productivity.

This included 40% of victims who stated they experienced a period of total work stoppage and complete loss of productivity.

Victims may feel the effects of these attacks for lengthy periods of time. Our data indicated 37% felt significant impact to their productivity for one to three months following the ransomware attack, and more concerning was that 50% of a victims' productivity was substantially impacted anywhere from four months to more than a year following a successful attack.

50% of ransomware victims reported productivity impacts of four months to a year following the attack.

In some cases, the total cost of this downtime and lost productivity can be higher than the ransom demand, putting decision makers into a difficult position of deciding whether it may be more cost effective to pay a ransom demand versus the time it may take to triage and recover without paying.

05

SECTION TWO: MITIGATION TRENDS

Multiple Next-Gen Endpoint Solutions in Use at Most Organizations

05 Multiple Next-Gen Endpoint Solutions in Use at Most Organizations

We have found that many organizations consider endpoint security tools to be one of the foundational elements of their security posture.

This is due to many factors, including the wide range of endpoint security technology, the capabilities and visibility these tools can provide, and the expansive reach they can have within a network. Therefore, our goal was to gain a better understanding of what approach environments are taking regarding their endpoint security strategy.

66% Our results found that 66% of organizations are currently using one or more next-generation endpoint security tools within their networks.

In our research we defined "next generation" as endpoint tools that have evolved beyond traditional antivirus, including EDR, EPP, or XDR technology. We found that some environments are still behind in the adoption of this technology, with 28% indicating that they are either using a traditional antivirus solution or are currently without an endpoint security solution of any kind. However, these respondents plan to purchase a next-gen endpoint solution within the next 12 months. The remaining 6% of respondents stated they currently have no plans to move to a next-generation solution within 12 months. Just as endpoint security technology is prevalent across networks, so are vendors.

87% Our results found that 87% of environments are currently using two or more unique endpoint vendor solutions.

The largest portion, 46%, currently acknowledge deploying two endpoint vendors within their network. This was followed by 28% of networks with three vendors, and an equal 13% of networks that are either using only a single endpoint vendor, or 13% of networks deploying four or more vendors within their environment.

06

SECTION TWO: MITIGATION TRENDS

Endpoint Visibility Gaps Persist as Agent Deployment Falls Short

SECTION TWO: MITIGATION TRENDS

06 Endpoint Visibility Gaps Persist as Agent Deployment Falls Short

As previously stated, endpoint security solutions are a key element of visibility and protection within most modern cybersecurity programs, but to achieve the best results from these tools it is crucial that an organization not only partners with a vendor that best fits their security needs, but also deploys these agent-based tools in totality to the endpoints throughout their network. This is because gaps in deployment of the endpoint agent can be seen as gaps in coverage, leading to areas of limited visibility and potential safe havens for threat actors to operate.

Our research found that 54% of environments have been unable to reach a complete, or 100%, deployment rate of the agent to all endpoints within their environment.

54%

Of the 46% that have managed to achieve complete deployment, 17% expressed that they are expecting to drop below this threshold and develop deployment gaps within the coming 12 months.

When we analyzed our results further, we found that 23% of environments achieved a current agent deployment rate to 90-99% of their total endpoints, 21% achieved an agent deployment rate to between 75%-89% of their total endpoints, and 10% of environments are at an agent deployment rate of less than 75% of their total endpoints.

06 Endpoint Visibility Gaps Persist as Agent Deployment Falls Short

Achieving and maintaining complete deployment within your network can be a complicated task, especially within large enterprise environments.

This further emphasizes the need for organizations to enhance their security visibility with multiple sources of telemetry, including network, cloud, log ingestion, identity sources, and more as this will provide redundancy in detection coverage if endpoint agent deployment gaps exist within your network.

These deployment gaps may be the result of numerous factors, one of which we identified in our research as the rate at which organizations choose to remove or replace their chosen endpoint vendor solutions.

We found that 70% of respondents made the decision to remove or replace an endpoint solution within their networks within the last 12 months, while only 4% of organizations have managed to go more than three years without removing or replacing an endpoint solution internally.

When asked what were the deciding factors that led to the replacement or removal of an endpoint vendor's product, we found a generally balanced range of responses.

These included difficulty in justifying price, lacking key required features, failures in detection, and more as indicated in the diagram, below.

Although these technologies have existed for over a decade, many environments are still in the process of updating or replacing security solutions as they look to achieve the proper fit for their environments.

Deciding factors for removing or replacing an endpoint solution

07

SECTION TWO: MITIGATION TRENDS

AI Usage Policies Become Priority

07

SECTION TWO: MITIGATION TRENDS

AI Usage Policies Become Priority

The utilization of large language models (LLMs) and generative artificial intelligence (GAI) has become an important topic of discussion within many organizations, as security decision makers find themselves in the difficult position of developing policies on their adoption and usage.

Leaders must consider the balance between the benefits these technologies may provide to their environment against the potential security and privacy risks that can arise.

In the Arctic Wolf Labs 2024 Predictions Report, our analysts predicted that the inclusion of vulnerabilities into AI-generated code will be a significant security concern this year.

Malicious users are already training these AI models to generate code that is vulnerable to exploitation. If an unsuspecting AI user places this vulnerable AI-generated code into production, it could result in it being used to carry out an attack.

07

SECTION TWO: MITIGATION TRENDS

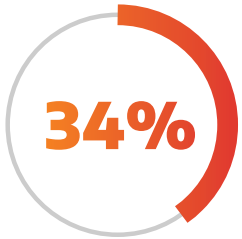
AI Usage Policies Become Priority

In addition, many security experts also warn of the privacy concerns associated with the usage of LLMs, as the input of a company's proprietary information or PII (personal identifiable information) by a user into one of these models is often considered a data breach, since this information can then be extracted by other users.

With all this information taken into account, we asked how security decision makers were approaching policy creation with respect to generative AI and large language models.

Our results found that 94% of organizations either currently have or plan to implement adoption and usage policies within the coming 12 months.

Of these, 49% currently have developed and implemented policies that outline the proper usage of LLMs and generative AI.



Another 34% have implemented policies which strictly forbid the use of these technologies within their environments.

We found that only 6% of organizations do not currently have plans to develop policies regarding these forms of AI, but this may change as these technologies continue to evolve and become more common.

Key Takeaway

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.

Arctic Wolf would advise any security leaders who find themselves in the minority of organizations who have no existing AI policies or plans to develop such policies to reconsider their position.

Artificial Intelligence shows signs of being a cornerstone of future technology development and any company that is not prepared to safely implement it will find themselves drastically increasing their overall threat risk.

08

SECTION TWO: MITIGATION TRENDS

Effectively Securing Cloud Resources

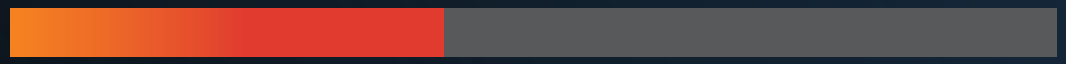
08

SECTION TWO: MITIGATION TRENDS

Effectively Securing Cloud Resources

Cloud security has been an important area of discussion within the last few years, with many organizations finding themselves in a position where cloud adoption has outpaced cloud security. The first important statistic we discovered in this area is that 99% of environments are using some form of public or private cloud. This rate of adoption aligns perfectly with similar research done in this area.

Despite this overwhelming majority who have cloud implementations, only 40% of organizations indicated that they are actively securing all their cloud resources effectively. This, unfortunately, shows the continued trend of the cloud being implemented by many organizations with security as an afterthought.



The results next show 44% of environments who are trying to secure their cloud resources but acknowledge that they are suffering some gaps. 12% were organizations who see their cloud implementation as a concern but are developing a plan to improve, and 3% of environments who admit that the cloud is the biggest single threat to their environment.

08 Effectively Securing Cloud Resources

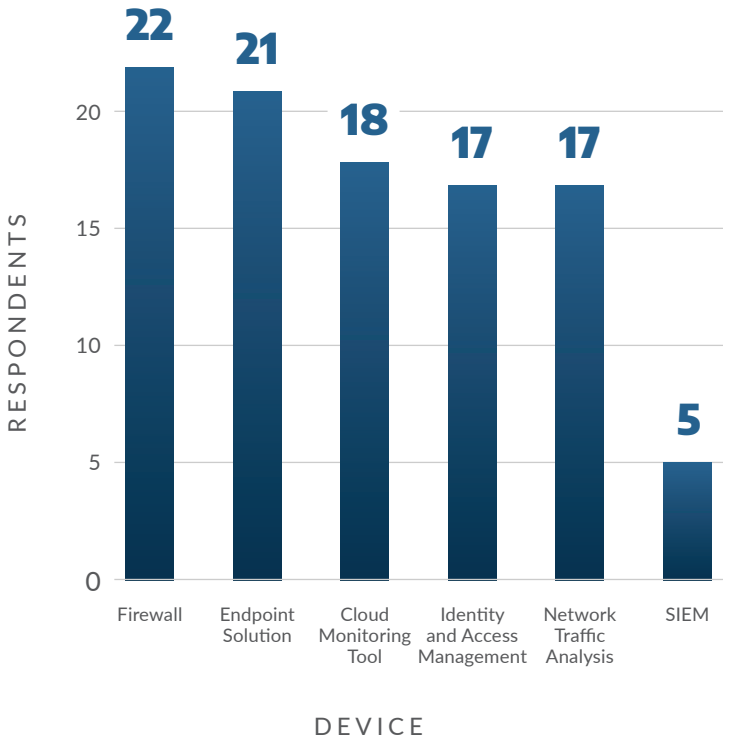
To effectively secure your cloud resources, you must have the necessary visibility into your cloud implementation, the proper threat intelligence to identify threats within cloud telemetry, and the human expertise to determine which cloud-based alerts are true positives and how to respond.

Unfortunately, due to the various styles of cloud implementation, the amount of cloud-generated traffic and data processing, and the number of cloud users an environment may have, some organizations experience a high rate of noise and alert fatigue based within cloud telemetry. However, this same concern can be attributed to almost any security device or source of telemetry within a network.

We asked decision makers to consider their security tool stack and tell us what they see as the tool or technology providing the least value in terms of alert quantity to alert quality.

What we found was a balanced distribution among the common technologies most environments deploy. This ultimately means that no single device can be seen as the culprit for "noise generation," rather quality of alerts may be unique to each environment.

It is therefore important to ensure organizations continue to employ multiple security technologies to achieve the greatest level of visibility, while pairing this with the proper human expertise to cut through the noise and identify true threats to the environment.



Devices with highest noise to value ratio

09

SECTION THREE: READINESS TRENDS

Organizations Recognizing the Value of Incident Readiness

SECTION THREE: READINESS TRENDS

09 Organizations Recognizing the Value of Incident Readiness

With the rate of data breaches growing annually, we sought to learn more about how well organizations are prepared to handle an incident if one occurs.

Our data shows that 64% of organizations have established a formalized incident response (IR) plan or established an incident response discretionary fund as part of their security program. This shows many organizations are actively preparing to respond if an incident is declared.

64%

It should be noted however that 13% of those with established IR plans admitted to not reviewing or updating their plan within the last 12 months. For an IR plan to be effective it should be reviewed for accuracy and updated based on any changes within the environment on a regular cadence.

What is an IR Plan?

IR plans consist of multiple documents and data sets that may be necessary to properly respond to a threat when one is identified.

Contact lists, areas of responsibility, disaster recovery plans, and more may be included in a formalized IR plan. Additionally, many of these plans also include information about a third-party incident response retainer if one was purchased by the organization.

09 Organizations Recognizing the Value of Incident Readiness

"If you had an emergency evacuation plan for your building developed and six months later the building had doors and windows removed and modified, but your plan was not updated, would you just hope in the case of an emergency that your team could easily evacuate by just figuring it out on the fly? A company's incident management plan is the roadmap during a crisis. Steps that are critical for both left and right of boom need to be defined and regularly updated when changes occur within your environment; yet even without changes, a plan should be regularly reviewed at minimum every six months to ensure execution can be seamless at a moment's notice."

- Kerri Shafer-Page, Arctic Wolf, Vice President of DFIR

Our research found that 64% of organizations have currently invested in an incident response retainer, with another 26% planning to obtain one within the next 12 months as an additional safety precaution in the event of a breach.

Of the organizations that have purchased an incident response (IR) retainer for their network, 70% acknowledged experiencing an incident that required them to utilize their retainer within the past 12 months.

Furthermore, 30% of IR retainer customers indicated their need to utilize the retainer two or more times within the last 12 months.

This 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 security program that decision makers are investing in to help quickly overcome security incidents.

10

SECTION THREE: READINESS TRENDS

Cyber Insurance Adoption Accelerates

10

SECTION THREE: READINESS TRENDS

Cyber Insurance Adoption Accelerates

Arctic Wolf has made significant investments in researching the current state of cyber insurance to better understand its adoption rate and how organizations plan to incorporate their policies within their overall security operations strategy.

In the 2023 Arctic Wolf Cyber Insurance Outlook Report, we found that cyber insurance was still a growing market with relatively recent adoption, and of those organizations who had a policy, 47% had only acquired their coverage within the last year.

In our current research we sought to confirm the continued adoption of cyber insurance within organizations of all sizes.

Our findings show the largest subset, 66% of respondents, are organizations who currently have an active cyber insurance policy.

Another 29% of companies stated they are either currently in the process of obtaining a policy or will seek to obtain one within the next 12 months.

10

SECTION THREE: READINESS TRENDS

Cyber Insurance Adoption Accelerates

This results in a total of 95% of all organizations planning to have a cyber insurance policy by next year, and only 5% who are either still hesitant about purchasing a policy or stuck in a position where they are unable to obtain coverage from a provider.

With this widespread adoption of cyber insurance, we wanted to know the biggest concern for organizations relating to cyber insurance.

We found 53% of survey respondents were most concerned with rising premiums and stricter requirements for maintaining coverage.

The unease around rising premiums was further echoed elsewhere in our results. When we asked our respondents to indicate what their urgent concern was with respect to their security strategy, 31% stated "increased cyber insurance costs" ranked highest among their concerns.

Furthermore, apprehension goes beyond only the financial aspects of maintaining a cyber insurance policy.

Our data found that 19% of respondents cited the time-consuming nature of the process for both obtaining and maintaining their policy as a primary concern of the cyber insurance process.

This indicates that, as we continue to see security decision makers adopt cyber insurance policies, it will not be without some level of concern and pain points.

11

SECTION THREE: READINESS TRENDS

Apparent Acceptance of the Skills Shortage

11

SECTION THREE: READINESS TRENDS

Apparent Acceptance of the Skills Shortage

In previous trend reports, Arctic Wolf found the security skills shortage to be both a primary concern and a motivating factor in the development of many organizations' security programs. Yet, this year we found an interesting shift.

When asked about the driving factors and urgent concerns organizations are focused on when developing their security strategy, we received a range of responses, with the highest result being 50% of organizations naming the protection and safeguarding of intellectual property and confidential data as their primary area of concern.

50%

This is understandably an important concern for many organizations, yet an equally interesting trend is how only 16% of respondents, the lowest percentage received, stated that the hiring and recruiting of security staff is one of their primary areas of concern.

In last year's The State of Cybersecurity: 2023 Trends Report, we found that 64% of organizations chose staffing related issues as the top concern keeping them from achieving their cybersecurity goals.

11

SECTION THREE: READINESS TRENDS

Apparent Acceptance of the Skills Shortage

This leads us to ask, "what has changed?" Has there been a sudden surge of talent available to meet the needs of most organizations, or have decision makers begun to accept the security skill shortage as a long-term problem and therefore started shifting their strategies to embrace alternative solutions?

Key Takeaway

"For years the cybersecurity industry has been focused on the security skills shortage and the challenge of hiring qualified professionals to protect your environment. This runs parallel to an increase in highly effective security operations services now available to buyers. As a result, many leaders have heard the message and are now accepting the struggles of hiring as a long term problem. What we see now is the trend of security decision makers pivoting and designing their security programs in ways that leverage these services so they no longer have to go without."

- Lisa Tetrault, Arctic Wolf, VP of Security Operations

SECTION THREE: READINESS TRENDS

12 How Organizations Are Addressing Employee Risk with Security Awareness

SECTION THREE: READINESS TRENDS

12 How Organizations Are Addressing Employee Risk with Security Awareness

Earlier in the report, we discussed the potential for insider threats and how not all of them are necessarily malicious. Instead, some may occur from users who are the victims of social engineering or as the result of risky behaviors from uneducated users. As such, the best way to prevent these situations from occurring is to make use of a security awareness program to educate your network users on security risks and proper system use.

Our data shows that 88% of organizations currently use some form of security awareness programs internally, with another 10% in the process of adopting such a program within the next 12 months.

This leaves only 2% of organizations stating they do not have plans to implement a security awareness program for their employees.

The fact that 98% of environments plan to have an awareness program by next year is a positive statistic, especially when coupled with the 25% of organizations who stated that "building a culture of security awareness" was a driving factor of their security strategy for the upcoming year, however we wanted to further research how organizations are implementing their awareness strategies.

12 How Organizations Are Addressing Employee Risk with Security Awareness

We found an even split of 44% of respondents who chose to develop their own security awareness program and another 44% who decided to purchase and implement an awareness program for their company. There is no harm in an organization taking the initiative to develop their own security awareness program for their employees, if they take the time to develop a quality program that reinforces key security concepts on a reoccurring, routine cadence.

Research in the area of learning and education has shown that, when hearing new information, humans forget 80% of what they have just learned after a month if this information is not reinforced. Therefore, it is important for these awareness programs to continually reinforce the important elements you want your users to remember.

Of those organizations currently using a security awareness program,

42%
make use of weekly topics and lessons,

51%
are on a cadence of monthly topics and lessons, and

7%
only require their users to engage in these lessons on a yearly basis.

If the average human forgets 80% of what they have learned after one month without reinforcement, how much of these security lessons will your users remember after 10-11 months?

Another important aspect of a security awareness program is the inclusion of a phishing simulation component. This element gives your users direct experience with identifying and reporting phishing attempts within your environment, helping to minimize the likelihood of a successful attack.

Among those who have a security awareness program, 77% are either currently using or are in the process of implementing a phishing simulation component within their program. This leaves 23% whose awareness program does not include phishing simulations.

These programs are relying solely on lessons or explanation to describe potential phishing emails to their users. While this is better than simply not educating your users on how to identify and report phishing attempts, it is not as effective at training and reinforcement as the hands-on approach of simulated phishing emails.

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 2024 and beyond.

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® 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.