netwrix

2024 Hybrid Security Trends

CONTENTS

EXECUTIVE SUMMARY

Netwrix Research Lab surveyed 1,309 IT professionals from 104 countries via an online questionnaire in February 2024 and compared the results to its Cloud Data Security Reports from 2022, 2020, and 2019 and its IT Trends Reports from 2023 and 2020. The resulting report will help organizations concentrate their security efforts on what really matters. Key findings include the following:

IT ARCHITECTURE

About 3 in 4 organizations have a hybrid IT architecture, as was the case in 2023. The share that have an on-premises-only infrastructure decreased slightly, from 19% to 15%. This tracks with last year's finding that 37% of on-premises-only organizations planned to adopt cloud technologies within 12 months.

SECURITY CHALLENGES

Employee mistakes or negligence topped the list this year, moving up from third place in 2023. Malicious actions by employees, however, remained near the bottom of the list.

SECURITY INCIDENTS

79% of organizations spotted a cyberattack within the last 12 months, up from 68% in 2023. In 2023, on-premises infrastructure suffered more cyberattacks; this year we saw almost identical results for both cloud and premises. Attacks associated with account compromise in the cloud keep gaining momentum: In 2024, 55% reported this type of incident compared to only 16% in 2020. Targeted attacks became more common on premises: 27% spotted this type of attack compared to 19% in 2023.

CYBERATTACK CONSEQUENCES

The share of organizations that suffered no impact due to security incidents dropped from 45% last year to 38% this year. The top negative consequence was unplanned expenses to address security gaps, cited by 45% of respondents in 2024 and 40% in 2023. 1 in 6 (17%) organizations estimated their financial damage from cyber incidents to be at least $50,000.

SECURITY MEASURES IN PLACE

Over the last year, organizations enhanced their security posture. The most notable progress was in identity governance: In 2024, 55% of respondents have this in the cloud and 58% have it on premises, as opposed to only 44% and 43%, respectively, in 2023. The survey also reveals that the main enhancements over the last year were made in the cloud rather than on premises.

PLANNED SECURITY MEASURES

Data classification topped the list of measures organizations plan to implement to improve cybersecurity, both on premises and in the cloud.

IT PRIORITIES

The main areas of concern are data security, network security and cybersecurity training. Interest in implementing AI tools surged from just 12% of respondents in 2020 to 28% in 2024. The share of organizations prioritizing cloud adoption keeps growing: It reached 36% in 2024, up from 32% in 2023 and 23% in 2020.

CYBER INSURANCE

62% of organizations have a cyber insurance policy or plan to purchase one within 12 months. Almost 1 in 5 (19%) insured organizations used their cyber insurance policy last year.

NETWRIX RESEARCH LAB EXPERTS

ILIA SOTNIKOV

Security Strategist and Vice President of User Experience at Netwrix

Ilia Sotnikov has over 20 years of experience in cybersecurity, as well as broad IT management experience. He is responsible for technical enablement, UX design and product vision across the entire Netwrix product portfolio.

Ilia's main areas of expertise are data security and risk management. He works closely with analysts from firms like Gartner, Forrester and KuppingerCole to gain a deeper understanding of market trends, technology developments and other changes in the cybersecurity landscape.

As a regular contributor at Forbes Tech Council, Ilia shares his knowledge and insights regarding cyber threats and security best practices with the broader IT and business community.

DIRK SCHRADER

Vice President of Security Research and Field CISO EMEA at Netwrix

Dirk is a 25-year veteran in IT security who works to advance cyber resilience as a modern approach to tackling cyber threats. He holds CISSP (ISC²) and CISM (ISACA) certifications.

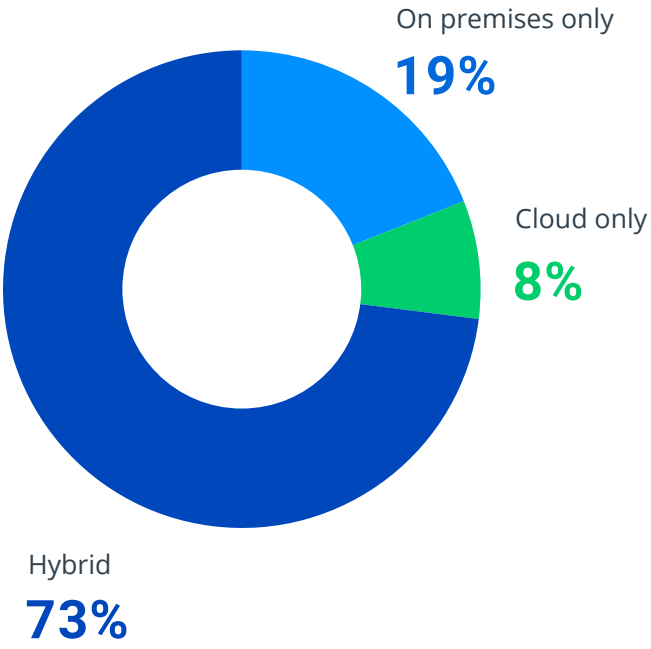
Along with general security research and vulnerability discovery, Dirk is keen on industry-specific focused research for verticals like healthcare, energy and finance. He has uncovered thousands of vulnerable systems at healthcare-delivering organizations around the globe and alerted those providers, authorities and the public.

Dirk has also published articles on topics such as cyber risk management, cyber resilience, and IT security tactics and operations.

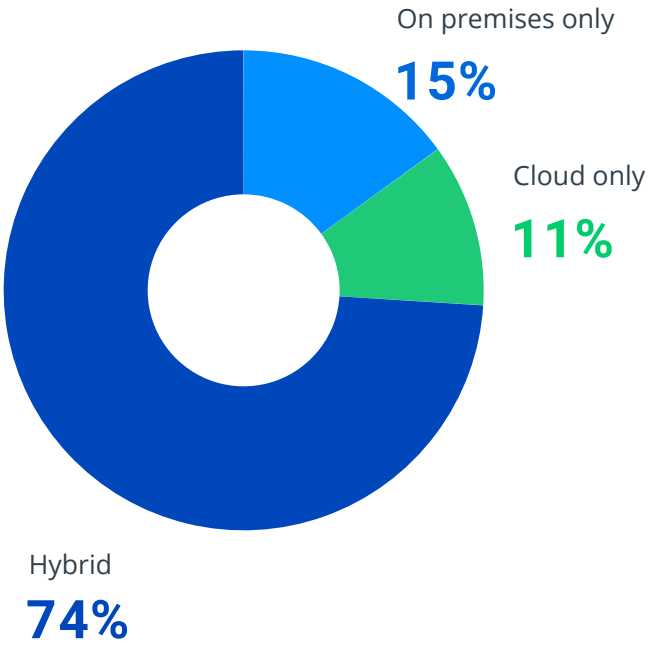
IT ARCHITECTURE

Remote and hybrid work, along with business needs for flexibility and cost efficiency, keep driving cloud adoption. About 3 in 4 organizations have a hybrid IT architecture, as was the case in 2023. The share that have an on-premises-only infrastructure decreased slightly, from 19% to 15%. This tracks with last year's finding that 37% of on-prem-only organizations planned to adopt cloud technologies within 12 months.

IT architecture (2023)

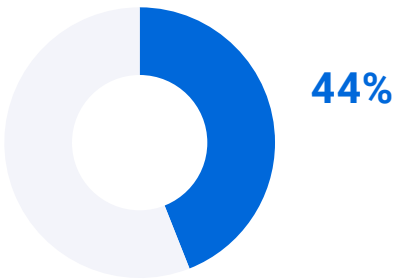


IT architecture (2024)

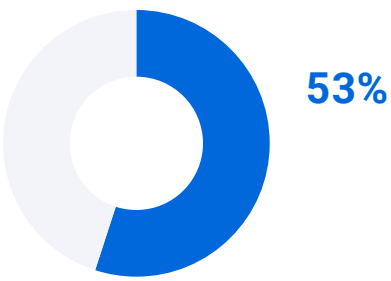


However, movement of workloads to the cloud progressed more slowly than respondents anticipated. The percentage inched up from 41% in 2022 to 44% in 2023 and then stayed flat in 2024, even though respondents expected it to reach 53–55%. This year's survey yielded a similar prediction, which indicates that IT pros are still looking to extend their cloud adoption.

Percentage of workloads already in the cloud (2024)



Percentage of workloads planned to be in the cloud 12 months from now (2024)



58% of on-prem-only organizations plan to adopt cloud technologies, and 30% plan to do so within 12 months

It's often hard to precisely predict project timelines for a major technological transition like cloud migration. Last year, in addition to the usual project planning challenges, organizations had to deal with the uncertainty of global economic headwinds. A good way to keep up the desired pace of cloud adoption is to break the cloud transition into stages that are easier to manage and control.

Ilia Sotnikov
Security Strategist
at Netwrix

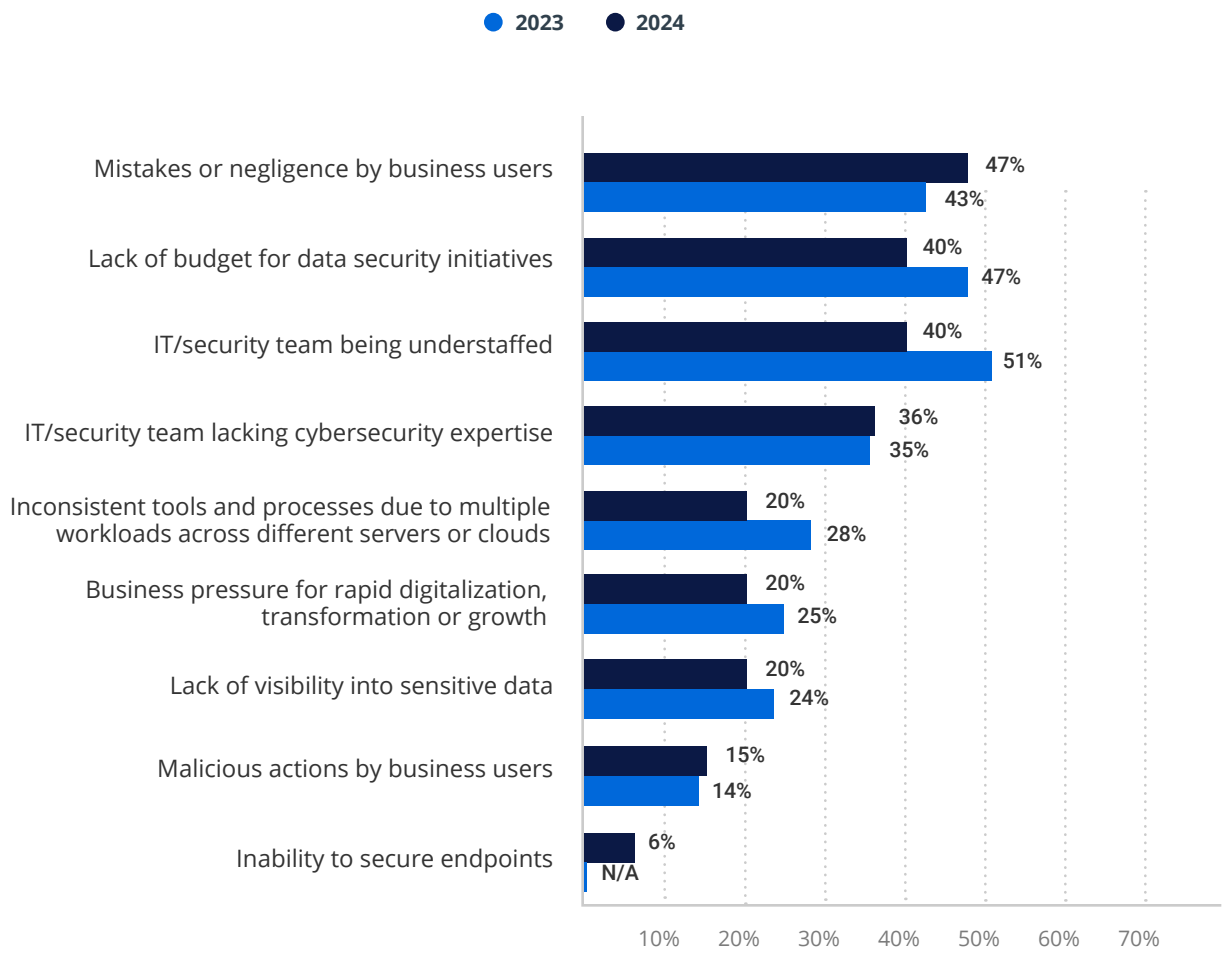
Cloud migration is a cyclic process that seemingly never ends. As an organization evolves, it re-evaluates which workloads need to be moved to the cloud or brought back on premises. The decision is usually based on factors like operational efficiency, costs, and compliance with the applicable laws and regulations. Workloads typically migrated to the cloud include those around HR, marketing and billing, as well as customer-facing processes that require seamless scaling.

Dirk Schrader
VP of Security Research
at Netwrix

SECURITY CHALLENGES

Ensuring data security is a tough job, but some obstacles are bigger than others. We asked our respondents to rank their top data security challenges. Employee mistakes or negligence topped the list this year, moving up from third place in 2023. Malicious actions by employees, however, remained near the bottom of the list.

Biggest challenges faced while trying to ensure data security (2023, 2024)



To address the top security challenge reported in the survey, security teams need to establish technical controls that help users avoid mistakes without significant inconvenience. User-friendly password management enables smooth yet secure logins, while judicious multifactor authentication helps prevent credential abuse without a heavy burden for employees. A modern privileged access management solution can provide just enough privilege just long enough to perform the task at hand, reducing the attack surface without introducing friction. Finding the right balance between security and a good user experience is the key to properly protecting the organization.

Dirk Schrader

VP of Security Research at Netwrix

We can expect tight budgets, understaffing and lack of security expertise to remain among the top concerns for IT security teams in the next few years at least. To address these challenges, organizations can seek ways to empower people to be more efficient. Frameworks such as NIST CSF and ISO 27001 help focus and prioritize security efforts. Organizations can also turn to the managed security service providers (MSSP) to close the skills or staffing gaps and leverage software solutions to automate labor-intensive tasks and reduce noise and false alarms.

Ilia Sotnikov

Security Strategist at Netwrix

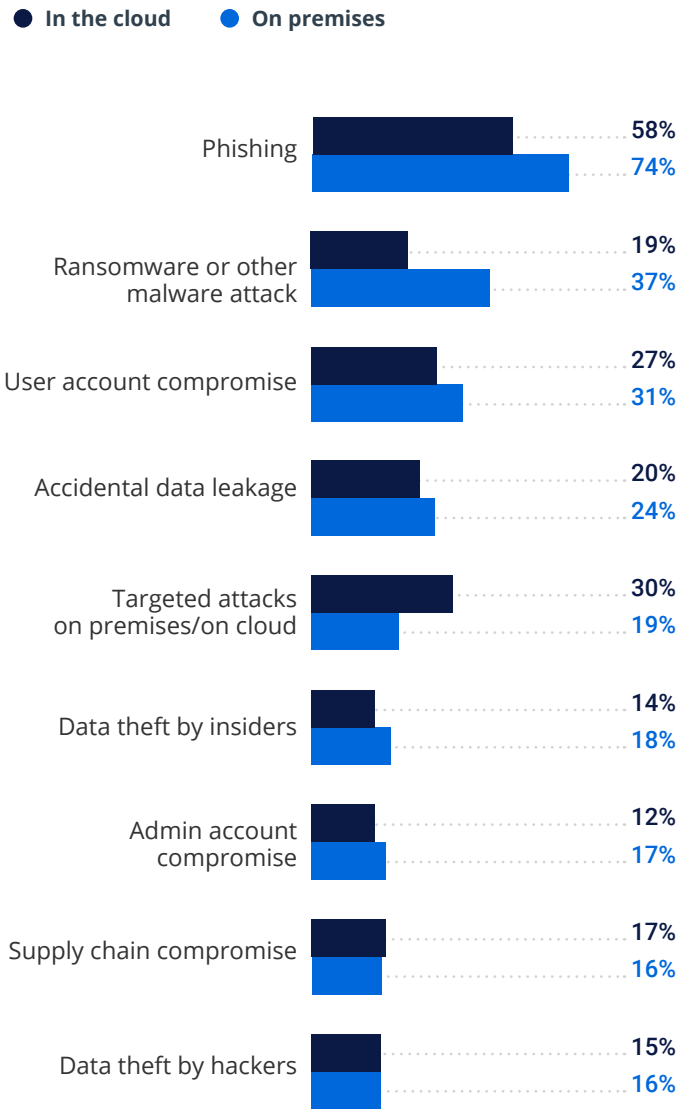
SECURITY INCIDENTS

79% of organizations spotted a cyberattack within the last 12 months, up from 68% in 2023.

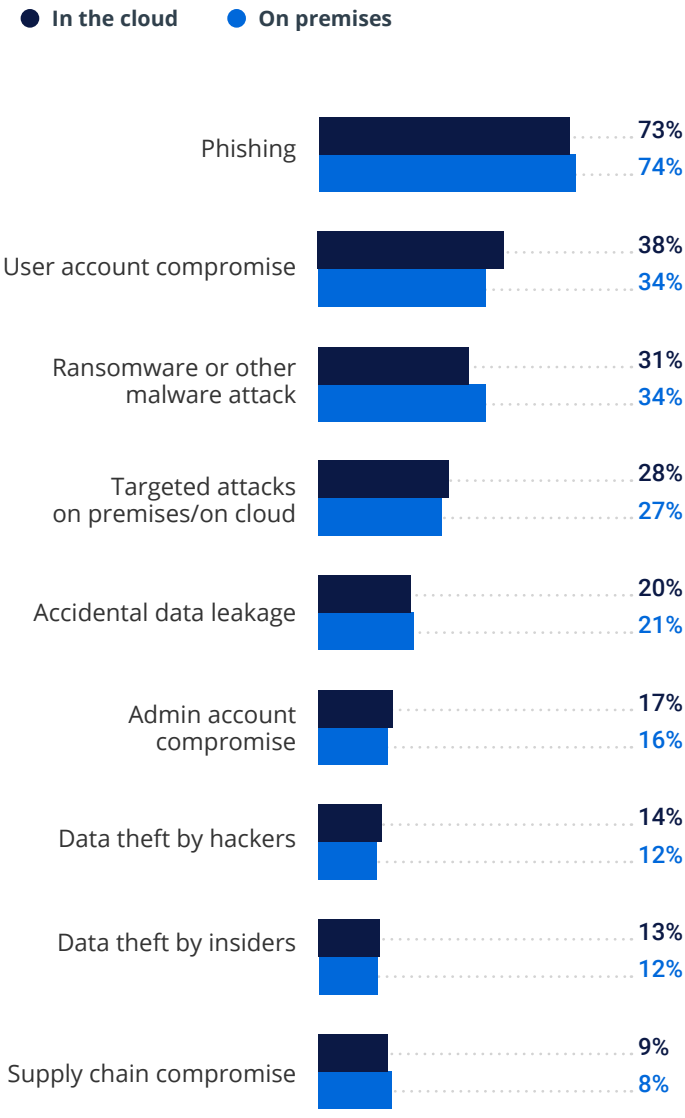
IN THE CLOUD VS ON PREMISES

We asked respondents whose organizations experienced a security incident to share details about the attack. In 2023, they reported more attacks on their on-premises infrastructures than the cloud, especially phishing and malware attacks. This year, however, the respondents reported almost identical results for both segments of their infrastructure.

Most common security incidents (2023)



Most common security incidents (2024)



Over the last year, cloud infrastructure became a more frequent target for attackers. Organizations keep adopting cloud technologies and moving their workloads to the cloud, although not at the anticipated pace. To increase the flexibility of the whole IT infrastructure, organizations opt to use third-party software-as-a-service (SaaS), platform-as-a-service (PaaS) and infrastructure-as-a-service (IaaS) technologies, or even develop them in-house. As a result, the attack surface in the cloud keeps growing — and so does the number of security incidents.

Dirk Schrader

VP of Security Research at Netwrix

This year, more organizations spotted an attack on their IT infrastructure. Off-the-shelf hacking tools, affiliate programs and a slew of cybercrime-as-a-service offerings are now empowering less-skilled cybercriminals to launch attacks. However, defenders are also upping their game with better detection capabilities, increasing the number of attacks that are identified. In addition, increasing recognition among executives about the business risks of security incidents is leading to more transparency, which also influences the number of reported incidents.

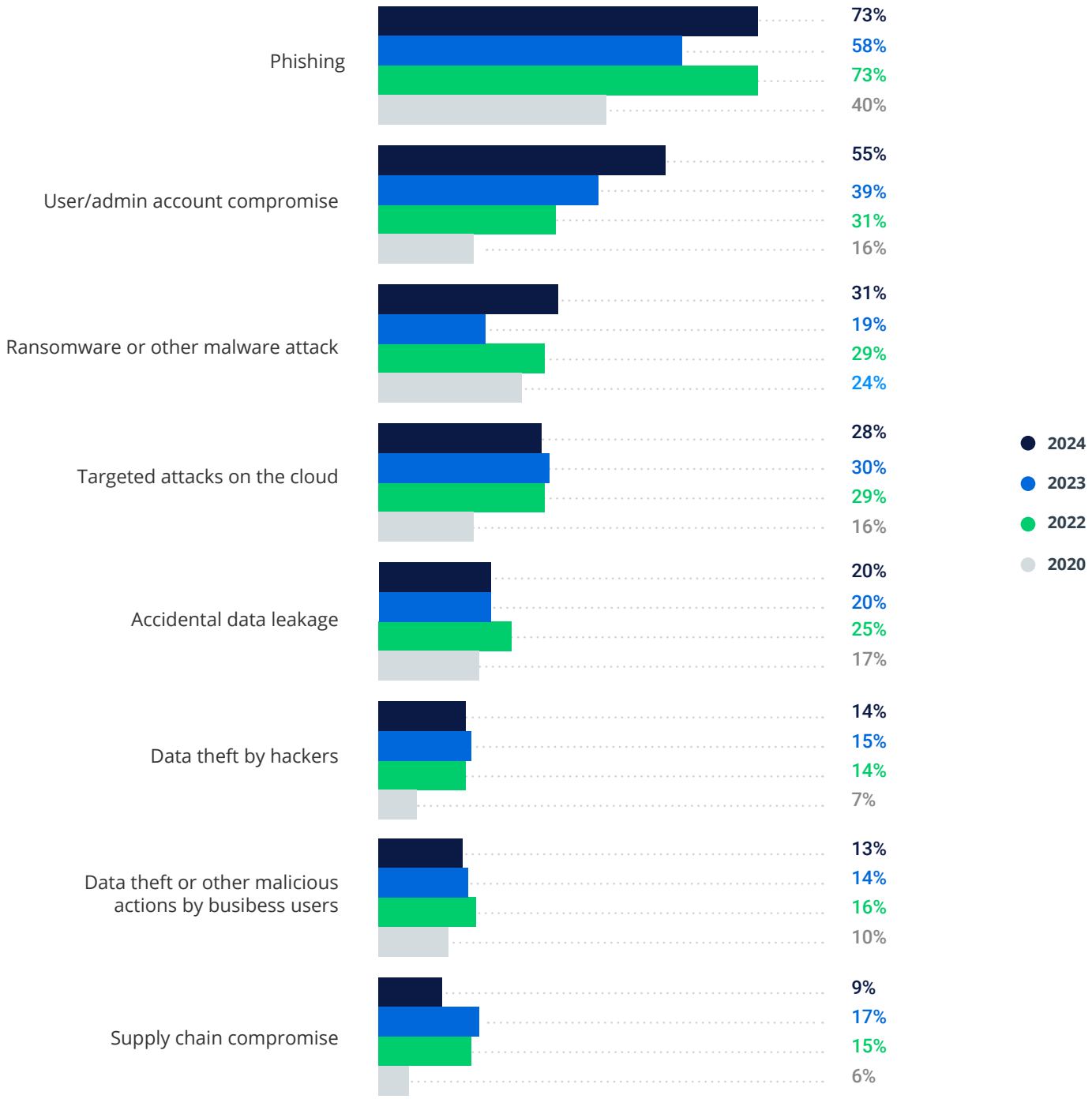
Ilia Sotnikov

Security Strategist at Netwrix

SECURITY INCIDENTS IN THE CLOUD

We compared this year's results regarding security incidents in the cloud to those from 2020, 2022 and 2023. While phishing remains the most common incident type, attacks associated with account compromise in the cloud keep gaining momentum: While only 16% of respondents reported this type of incident in the cloud in 2020, this percentage soared to 55% in 2024.

Most common security incidents in the cloud (2020, 2022, 2023, 2024)



Implementation of third-party SaaS or in-house cloud solutions significantly increases the number of identities in use, so it's no wonder that attacks associated with admin and user account compromise keep intensifying. To address this risk and reduce the attack surface, it is crucial to stick to the least privilege principle and ensure identity governance so that each user has just enough rights to do their job. Organizations should also consider enforcing multifactor authentication (MFA) for all accounts accessing in-house cloud solutions, just as cloud service providers usually require by default. If the in-house solution is a customer-facing application, MFA is a must-have.

Dirk Schrader

VP of Security Research at Netwrix

The survey trends confirm what industry experts have been saying for years: Identity is the new perimeter. Attackers will continue to target them and — sooner or later — succeed. IT security teams should seek a balanced approach to securing accounts. In addition to implementing the least privilege principle, they can reduce the risk of account compromise with multifactor authentication, single sign-on and user awareness training.

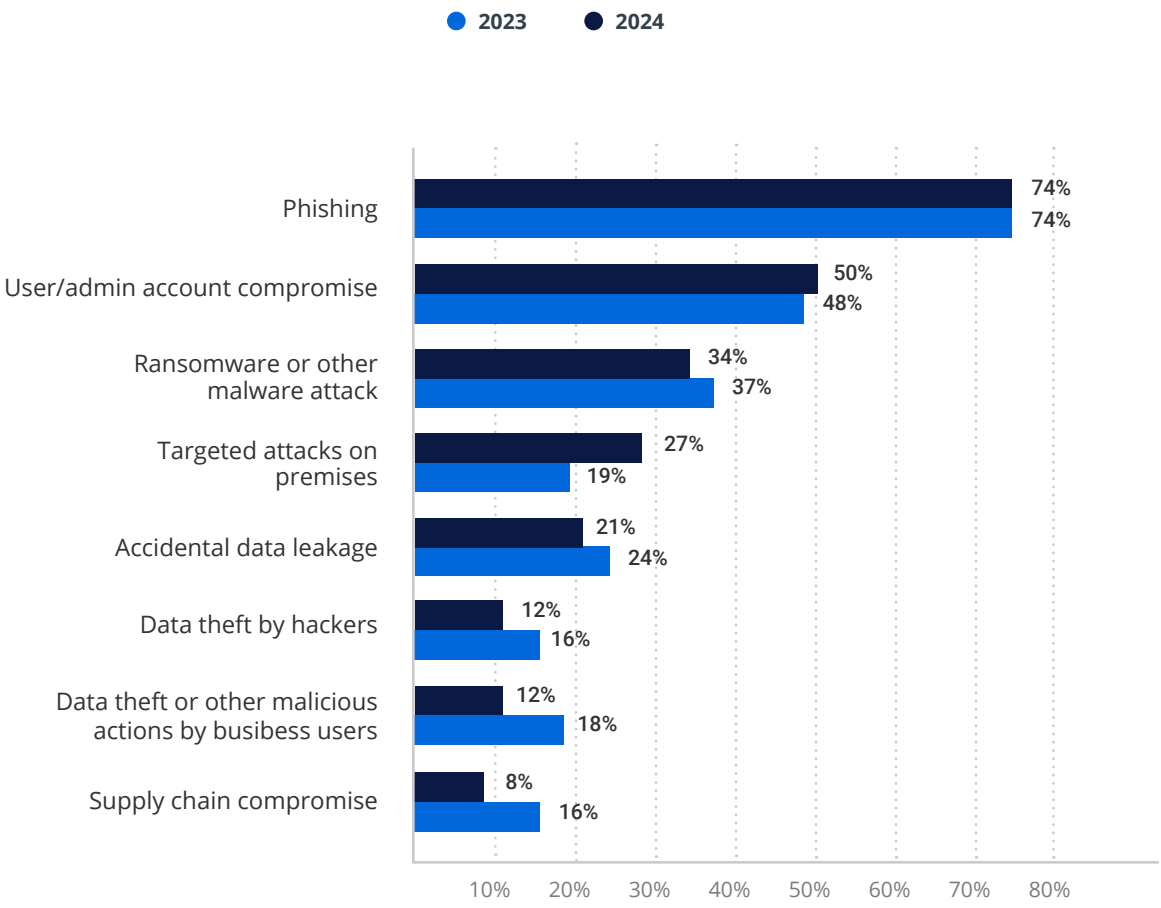
Ilia Sotnikov

Security Strategist at Netwrix

SECURITY INCIDENTS ON PREMISES

To understand security incident trends on premises, we compared the results from our 2023 report with the data collected in 2024. Notably, the share of those who suffered a targeted attack increased by 42%, from 19% to 27%.

Most common security incidents on premises (2023, 2024)



Non-targeted campaigns are easier to identify and address, for both security teams and regular business users. Accordingly, attackers are shifting to an individual approach. Moreover, targeted attacks are now easier to craft: Powered with AI, cybercriminals collect and analyze data from previous data breaches, social media and other publicly available information to adjust their malicious campaigns to specific sectors, organizations or even individuals. However, while targeted attacks increase the chance of initial infiltration, they unfold just like all the others: privilege escalation aimed at getting access to sensitive data.

Dirk Schrader

VP of Security Research at Netwrix

Historically, on-premises environments have better-established security controls and processes. Teams are more experienced, and technology changes are slower than in the cloud. As a result, on average, organizations with on-prem workloads are better prepared to thwart drive-by compromise attacks. Adversaries who are financially or politically motivated to attack such environments see lower success rates with a "one-size-fits-all" approach and are forced to find a more targeted approach to these organizations.

Ilia Sotnikov

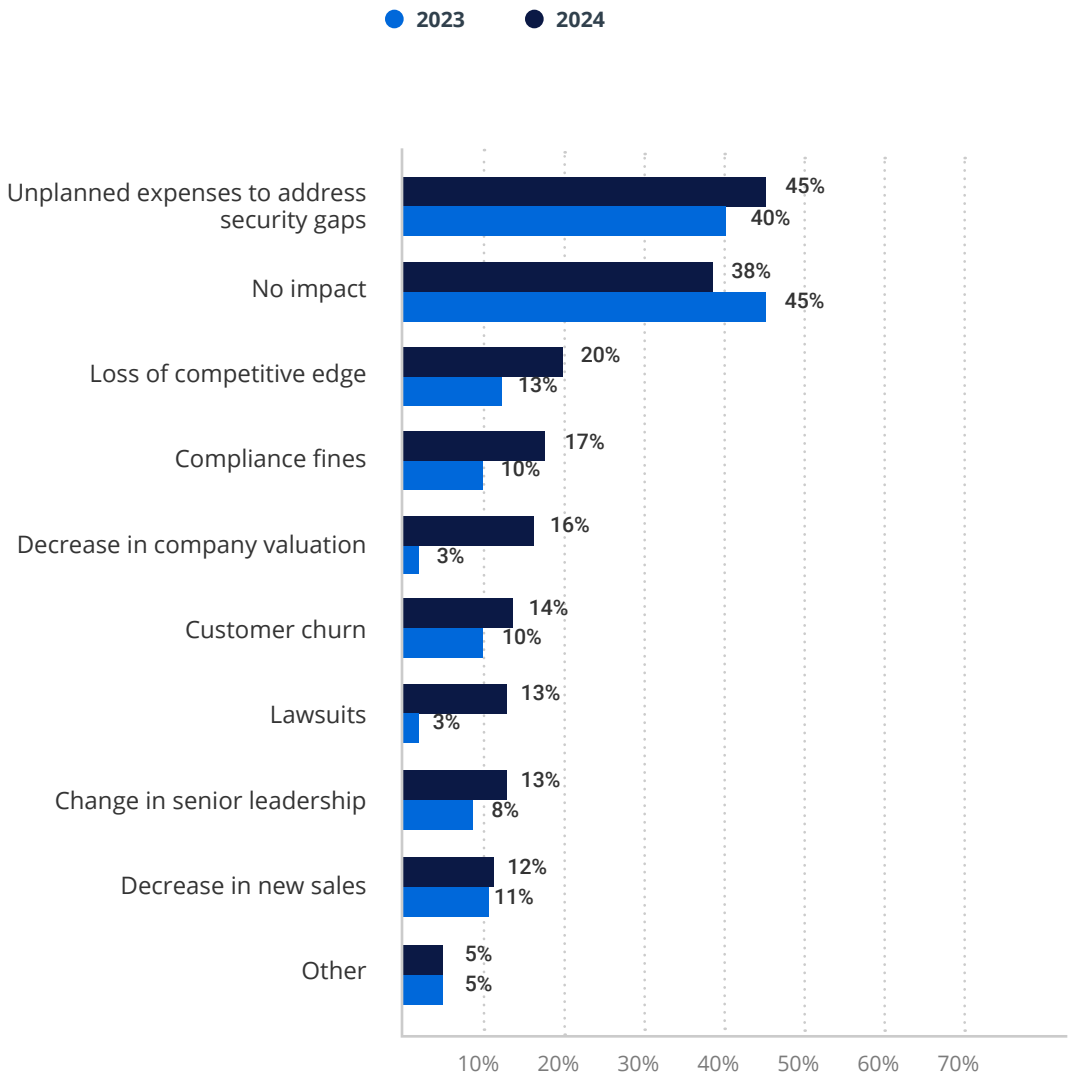
Security Strategist at Netwrix

CYBERATTACK CONSEQUENCES

Not every cyberattack results in damage, but the share of organizations that suffered no impact due to security incidents dropped from 45% last year to 38% this year. The top negative consequence was unplanned expenses to address security gaps, cited by 45% of respondents in 2024 and 40% in 2023.

Other impacts include damage to the company's competitive edge, valuation or revenue stream, and compliance and legal costs. In fact, this year, significantly more organizations reported many of these additional consequences.

Cyberattack consequences (2023, 2024)



1 in 5 organizations report losing a competitive edge due to a cyberattack.

Growing security awareness at the executive level means a better understanding that the risks of security gaps extend far beyond downtime and data loss. As a result, more organizations are investing resources into external or internal audits to find, analyze and remediate the root cause of a security incident to prevent similar events in the future. Mitigation measures can range from simple system configuration changes to large projects like data discovery and classification or redesign of identity access management.

Ilia Sotnikov

Security Strategist at Netwrix

An incident can reveal security gaps such as excessive admin privileges, dormant accounts, weak or unchanged passwords, default passwords or configurations, and unpatched systems. Fixing a gap might not require spending additional money but will definitely require time from the IT security team. In other words, addressing the root cause of a security incident results in additional investment, in either money or effort.

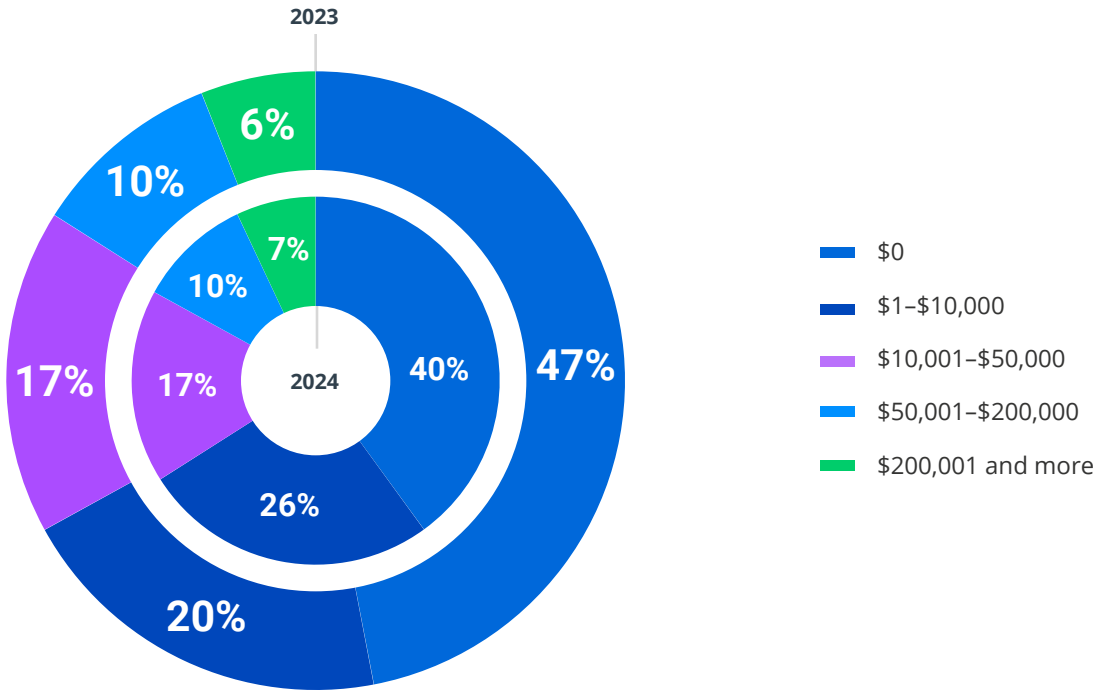
Dirk Schrader

VP of Security Research at Netwrix

SECURITY INCIDENT COSTS

Even though not every attack results in financial damage, some can be quite costly. Indeed, 1 in 6 (17%) organizations estimated their financial damage from cyber incidents to be at least $50,000. What's more, compared to last year, the share of those who faced no financial consequences due to security incidents dropped from 47% to 40%.

Cost of security incidents (2023, 2024)

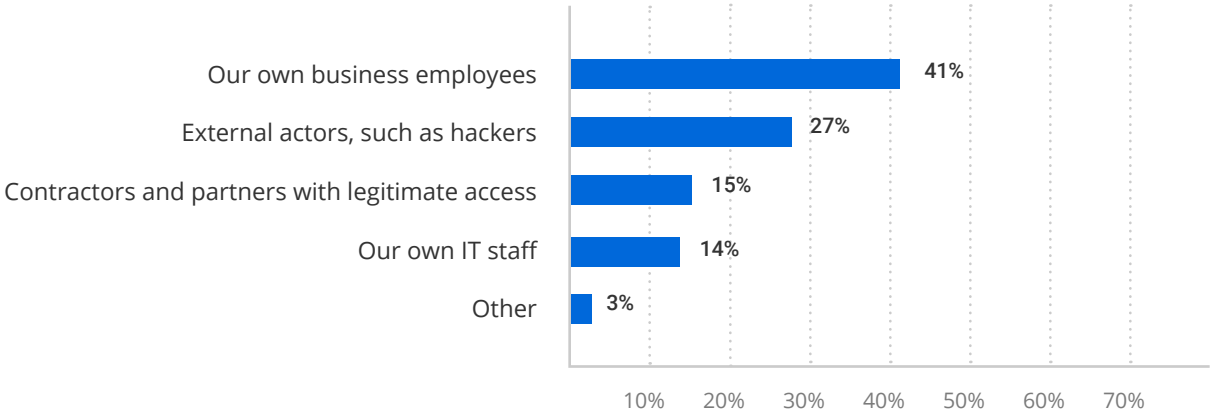


1 in 6 organizations reported at least $50,000 in financial damage from cyber threats.

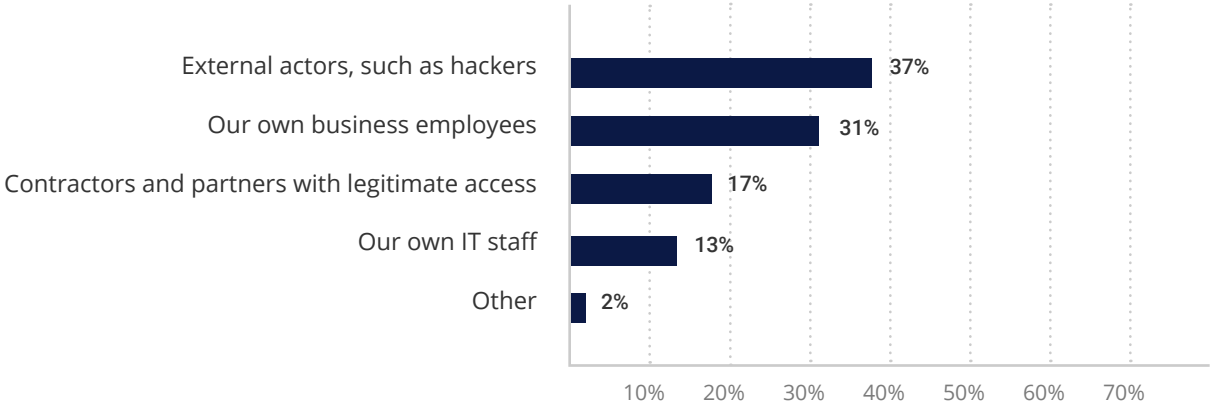
THREAT ACTORS

Assessing who is a threat is crucial to building an effective security architecture. We asked respondents to choose the single type of actor that poses the biggest risk to their organization's data security. It turns out that IT pros are most concerned about their own employees when considering on-premises infrastructure, while external adversaries topped the list for the cloud.

Who poses the biggest risk to data security on premises (2024)



Who poses the biggest risk to data security in the cloud (2024)



Threats from business users usually involve mistakes or negligence, rather than malicious actions. The best approach to mitigating the associated risks is to implement guardrails for end users and admins that keep mistakes from causing serious consequences. The first step is to gain complete visibility into data and assigned privileges. Then, review those access rights and remove all excessive privileges — and repeat this review step regularly. To shrink the attack surface even further, organizations can implement a privileged access management (PAM) solution that provides just-in-time privileges.

Dirk Schrader

VP of Security Research at Netwrix

Cloud service providers bear a part of the responsibility for security, but organizations must understand how responsibilities are shared. They need to know what kind of assurance is offered and determine whether it is adequate for the business risks. Sometimes, good customer reviews and peer references will be enough. More often, organizations need third-party validation, such as certifications, access to audit results or commitment to periodic penetration testing. In high-risk scenarios, organizations may require first-hand access to audit the provider's infrastructure and participate in red-team exercises.

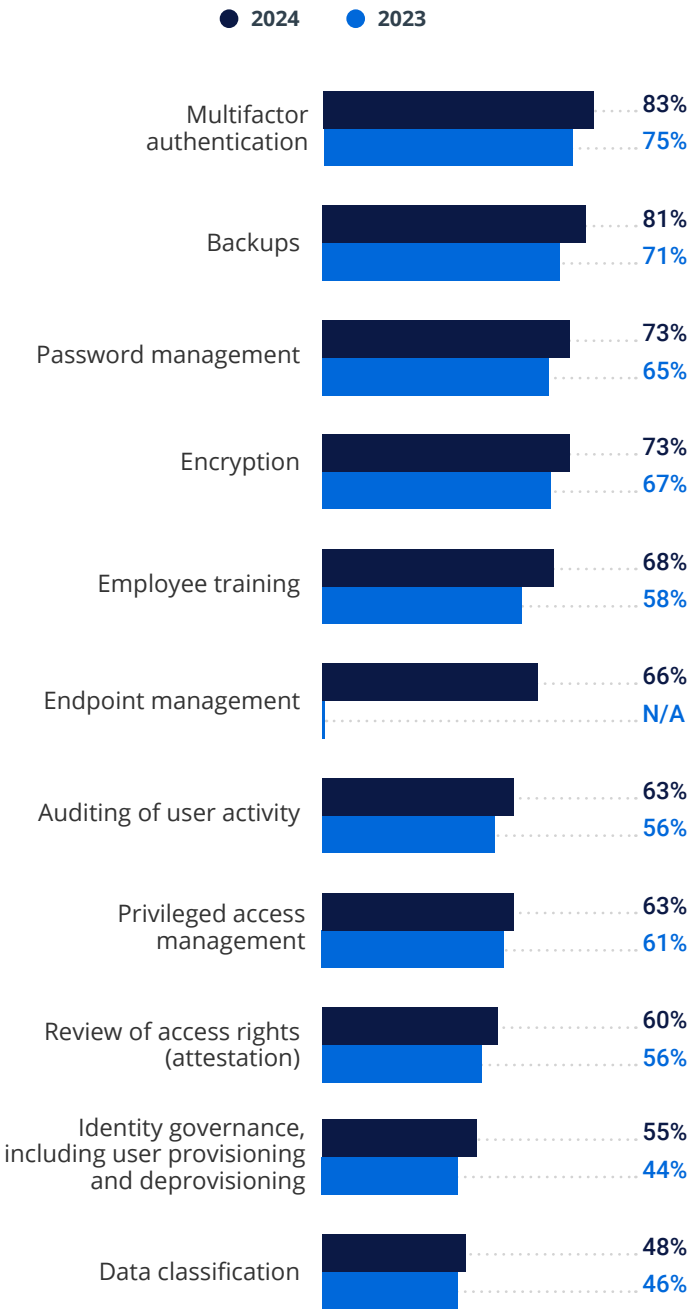
Ilia Sotnikov

Security Strategist at Netwrix

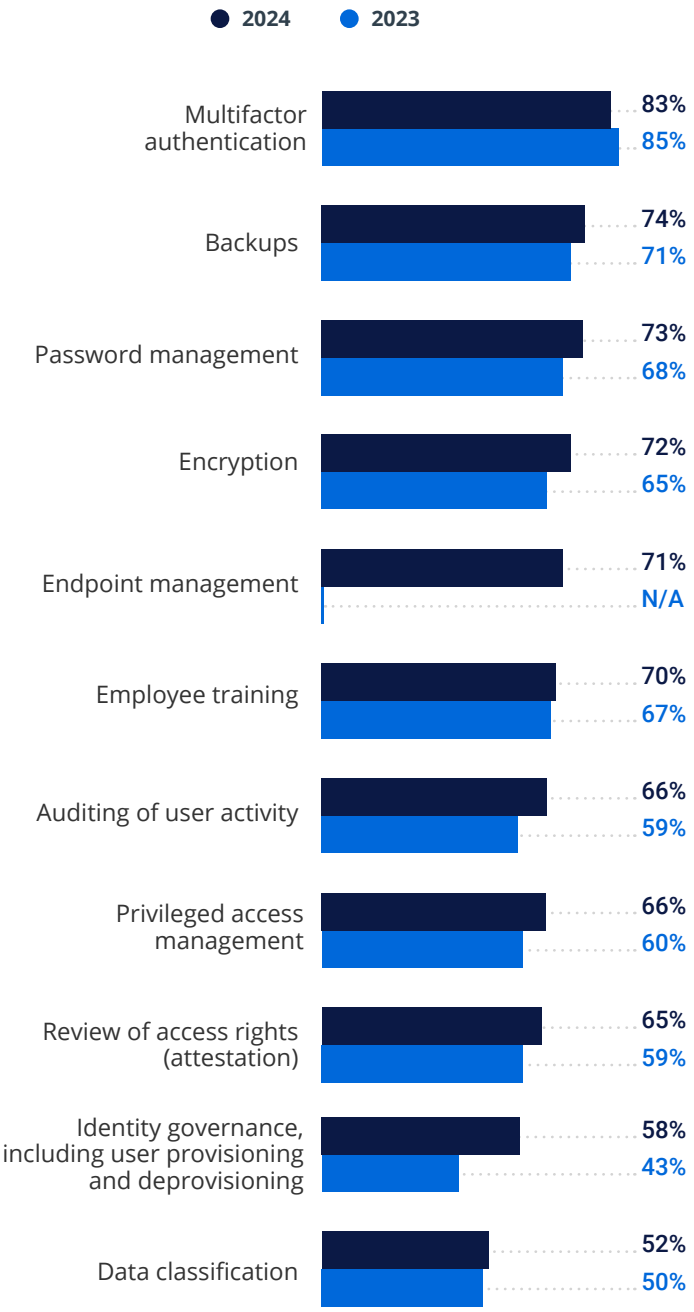
CURRENT SECURITY MEASURES

We asked our respondents what measures they take to protect data in the cloud and on premises. In comparing the results with last year's survey, we discovered that overall, organizations had enhanced their security posture with additional security measures. The most notable progress was in identity governance: This year, 55% of respondents have this in the cloud and 58% have it on premises, as opposed to only 44% and 43%, respectively, in 2023. The survey also reveals that the main enhancements over the last year were made in the cloud rather than on premises.

Measures already taken to protect data in the cloud



Measures already taken to protect data on premises



An identity governance solution streamlines the management of user identities and their access to data and other IT resources. This visibility and control facilitates the configuration of other security solutions and helps organizations map out further necessary enhancements to the security architecture.

Dirk Schrader

VP of Security Research at Netwrix

Only 51% of fully cloud-based organizations have a PAM solution in place, compared to 63% in general.

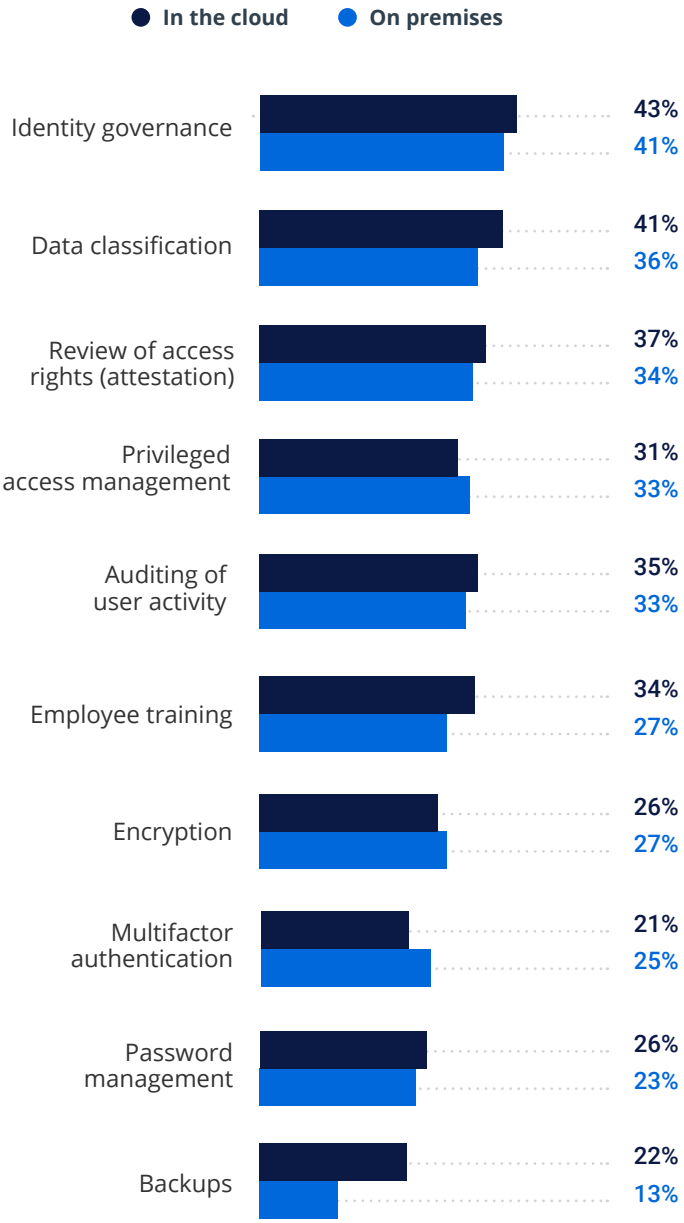
Only 47% of fully on-premises organizations have an IGA solution in place, compared to 58% in general.

PLANS FOR FUTURE SECURITY MEASURES

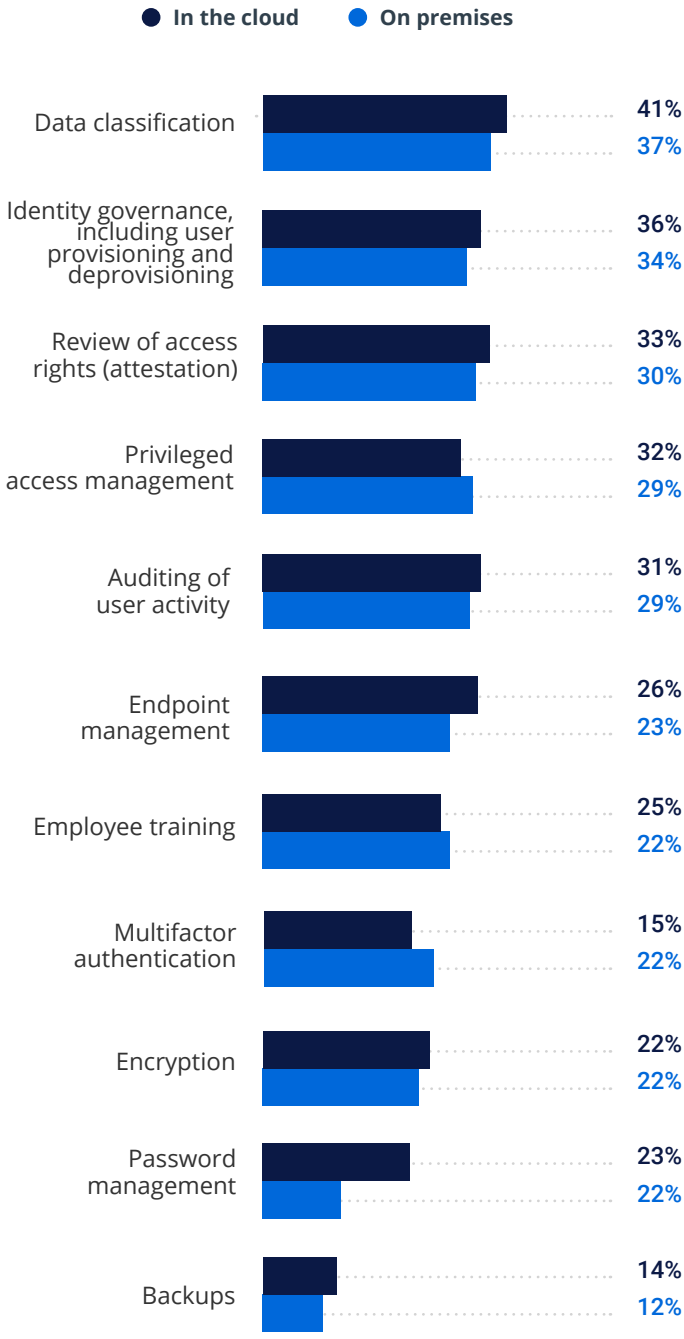
ORGANIZATIONAL PRIORITIES

This year, data classification topped the list of measures organizations plan to implement to improve cybersecurity, both on premises and in the cloud. As noted earlier, the share of those who have adopted identity governance rose compared to 2023, so it is not surprising that this measure moved from first to second place on the 2024 ranking.

Cybersecurity measures planned by organizations (2023)



Cybersecurity measures planned by organizations (2024)



Cloud adoption spurred IT security teams to switch their focus away from securing the network perimeter, which had become blurry, to identity as the new perimeter. Identity governance, review of access rights and privileged access management (PAM) all help ensure that the right users have the right access to the right things at the right time. Automating these processes saves valuable IT team time and improves accuracy, yielding a resilient and agile security posture.

Dirk Schrader

VP of Security Research at Netwrix

Data classification remains the top measure organizations plan to add to their security arsenal. Still, only half of organizations have actually implemented it. The main challenge is the effort required in manual approaches. Indeed, it's business users who know best what type of information is in the document they are attaching to an email or copying to a shared location. But manual classification simply isn't scalable because it requires a massive investment of time that creates barriers to user productivity. Moreover, it is highly inconsistent and extremely prone to user error. Automated classification addresses these challenges. Keep in mind, however, that it requires close collaboration between departments to tune the systems and processes to meet changes to business and legal realities.

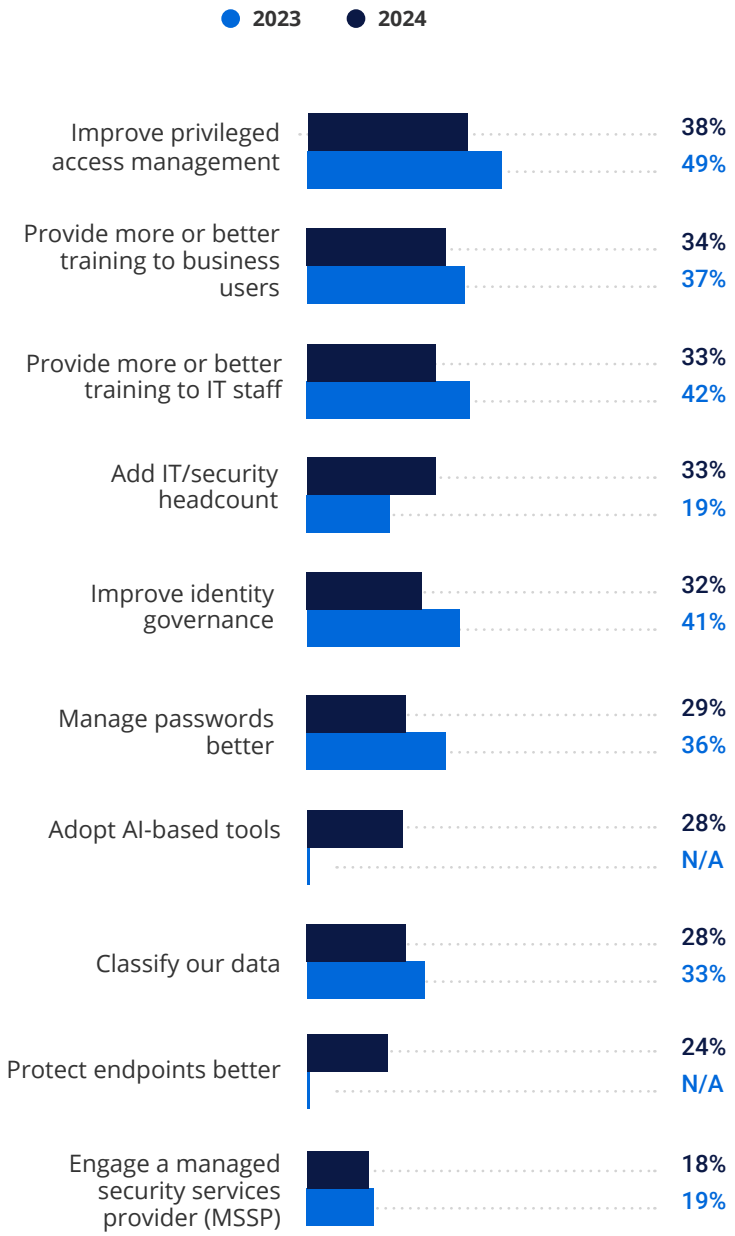
Ilia Sotnikov

Security Strategist at Netwrix

IT PRO PRIORITIES

Like last year, we asked our respondents what enhancements they would implement if they could choose how to improve their organization's security posture. PAM is still at the top of the list, followed by training for IT staff and regular business users. However, interest in other security measures dropped and is now spread more evenly. Interestingly, 33% of respondents in 2024 would add IT/security headcount, up from only 19% a year ago.

Cybersecurity measures that IT pros would prioritize (2023, 2024)



Growth in cloud adoption and the fast pace of changes in the cloud make the staff shortage issues more acute year over year. IT professionals are looking for ways to balance the load better so they are naturally considering implementing generative AI and large language models (LLMs). The world is still climbing to the peak of inflated expectations around these technologies, and AI will not solve all the problems. Organizations should stay pragmatic: AI-powered solutions can help in some cases, but they won't replace the need for proper security governance and basic security hygiene.

Ilia Sotnikov

Security Strategist at Netwrix

BROADER IT PRIORITIES

No organization has limitless human and budget resources, so prioritization is vital, including for security and IT teams. We asked respondents about their organization's top IT priorities for 2024. We compared the results with those from 2020 (when lockdowns were in full swing) and 2023 (when remote and hybrid work had become the new normal).

The main areas of concern stayed the same: data security, network security and cybersecurity training. Interest in implementing AI tools surged from just 12% of respondents in 2020 to 28% in 2024. The share of organizations prioritizing cloud adoption keeps growing: It reached 36% in 2024, up from 32% in 2023 and 23% in 2020.

When considering AI solutions, it is essential to start with a realistic goal of accelerating business processes without jeopardizing security. To identify the processes that are most suitable for automation, organizations should ask the following questions:

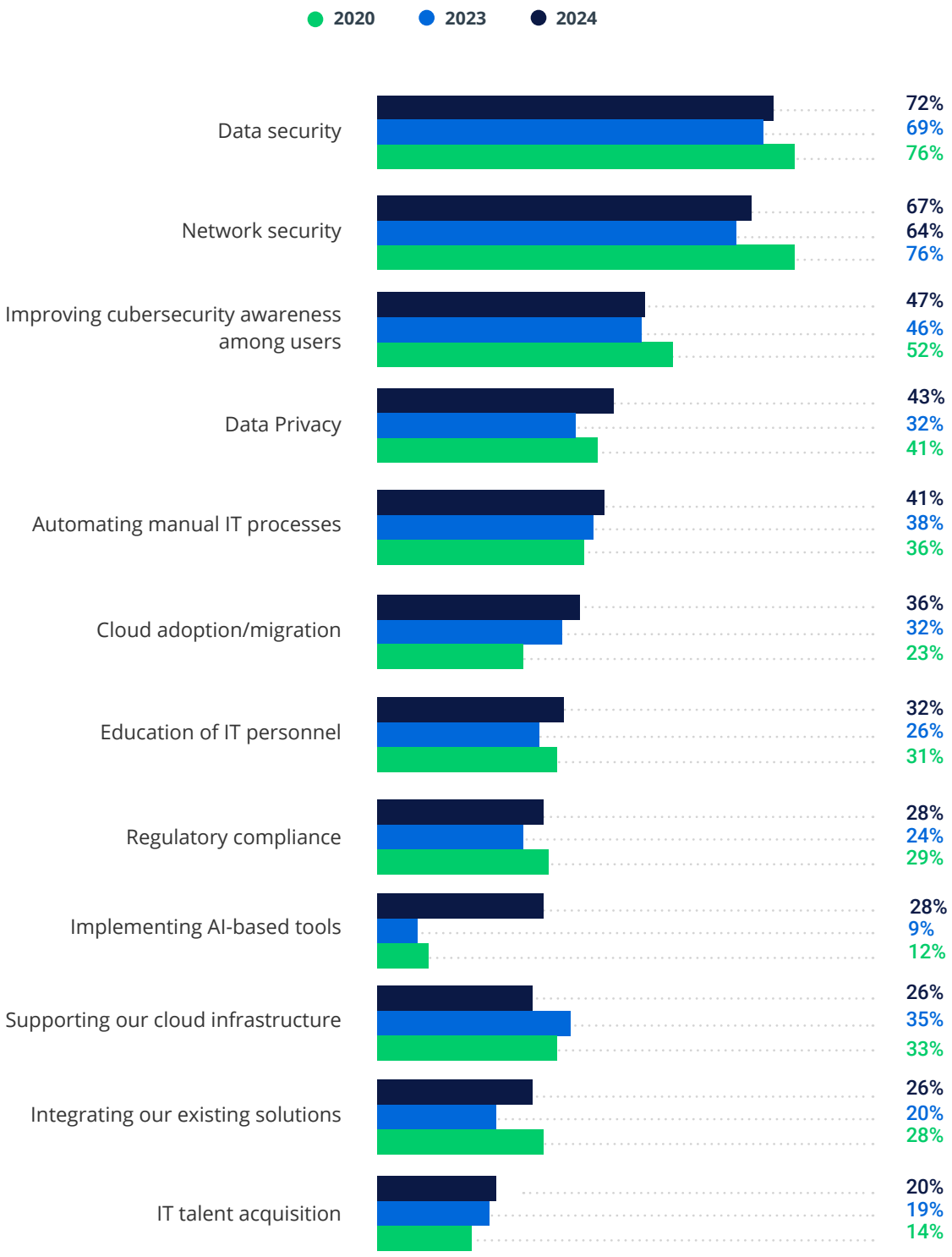
- **Is the process repetitive and time-consuming to do manually?**
- **Is the process sufficiently well defined to be turned into an algorithm?**
- **Does the process deliver verifiable results so a person can determine if something was wrong?**

Using these screening questions helps ensure that AI will be applied to increase the efficiency and accuracy of processes while keeping outcomes under control.

Ilia Sotnikov

Security Strategist at Netwrix

Organizational IT priorities (2020, 2023, 2024)



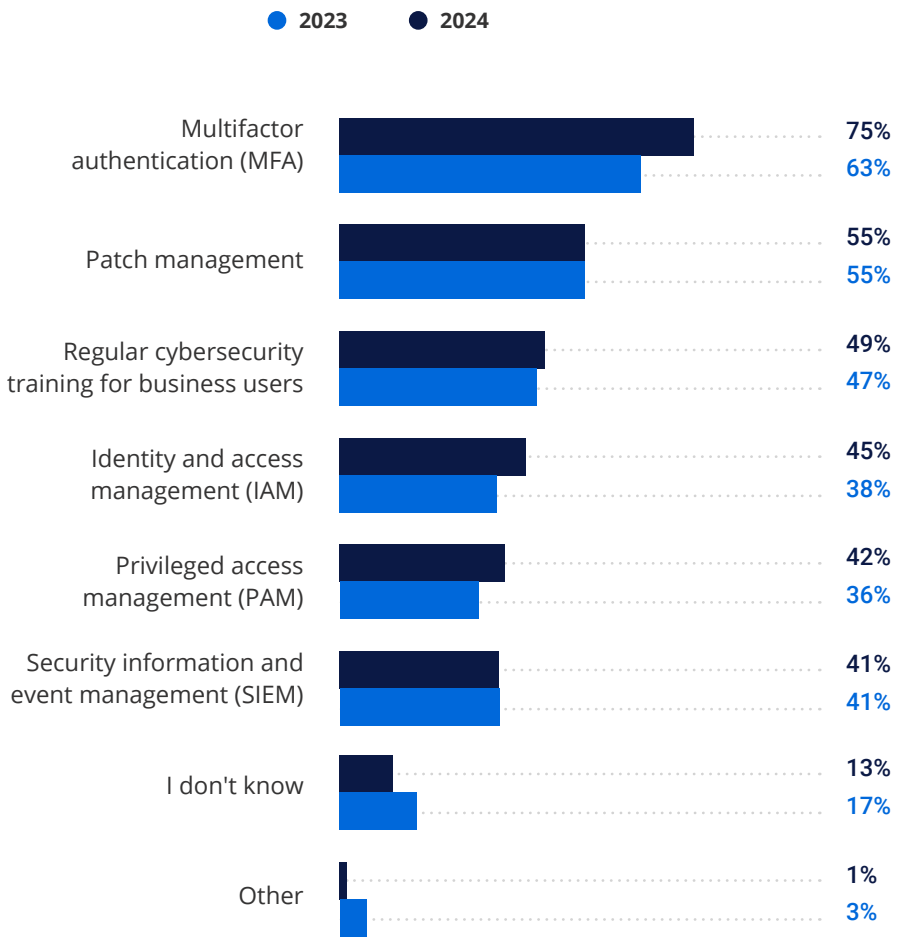
CYBER INSURANCE

No cyber insurance policy can restore an organization's data or operations in the wake of an incident, but an insurance payout can defray the financial impact and even prevent bankruptcy. This approach to risk management is quite popular: 43% of organizations are insured, and 19% plan to purchase a policy within the next 12 months.

INSURER REQUIREMENTS

Like last year, we asked respondents with cyber insurance what requirements they had to meet in order to qualify for a policy. While the top measures stayed the same, it turns out that insurance companies are now more likely to require identity and access management (IAM) as well as privileged access management (PAM). In addition, 75% of insured organizations had to have MFA in place in 2024, up from 63% in 2023.

What requirements did your organization have to meet for the insurance company to issue the policy? (2023, 2024)



62% of organizations have a cyber insurance policy or plan to purchase one within 12 months, up from 59% in 2023.

One thing insurance providers understand really well is risk management. They know that, sooner or later, adversaries with enough motivation and resources will break into an IT environment. PAM makes it harder for attackers to move laterally through the environment and escalate their privileges, and it ensures they will create more noise along the way. All this gives defenders more opportunity to detect and respond to attacks in time to prevent significant losses. And minimizing the loss (e.g., the payout) is exactly what insurance providers are looking for.

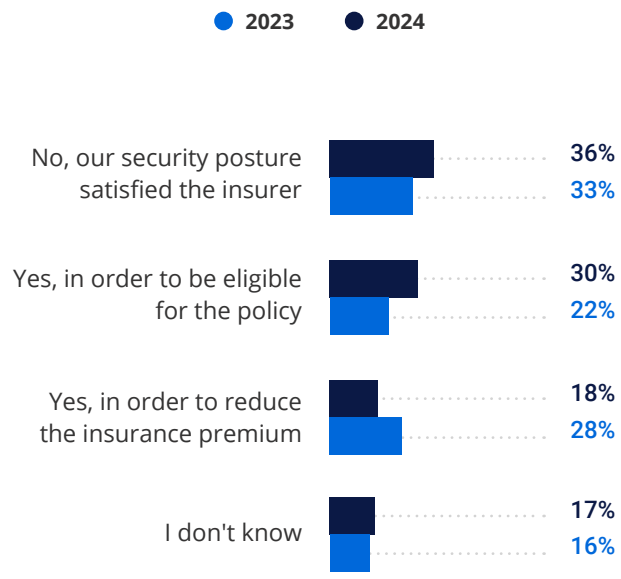
Ilia Sotnikov

Security Strategist at Netwrix

CHANGES NEEDED TO OBTAIN A POLICY OR REDUCE ITS COST

As in 2023, almost half (48%) of the organizations had to make changes to their security posture to meet the criteria of the insurance policy they chose. However, a more detailed analysis shows that insurers tightened their requirements over the last year. Indeed, the share of those who had to implement additional security measures just to be eligible for the policy increased from 22% to 30%, while only 18% made such changes to reduce the insurance premium, down from 28% last year.

Did you make any changes to meet the requirements of the insurance policy? (2023, 2024)



The most effective security controls are those aligned with the usual attack path. First, attackers will try to get their foot in the door by exploiting vulnerabilities or by utilizing phishing or password attacks to gather user credentials. To thwart them, make sure you have strong password management and MFA in place. Attackers who manage to slip into the network will attempt to move laterally and compromise privileged identities. Therefore, PAM must also be a priority. The final stage of the attack is to steal data or impair systems, so locked down access to sensitive data as well as backup and recovery capabilities in place are also essential.

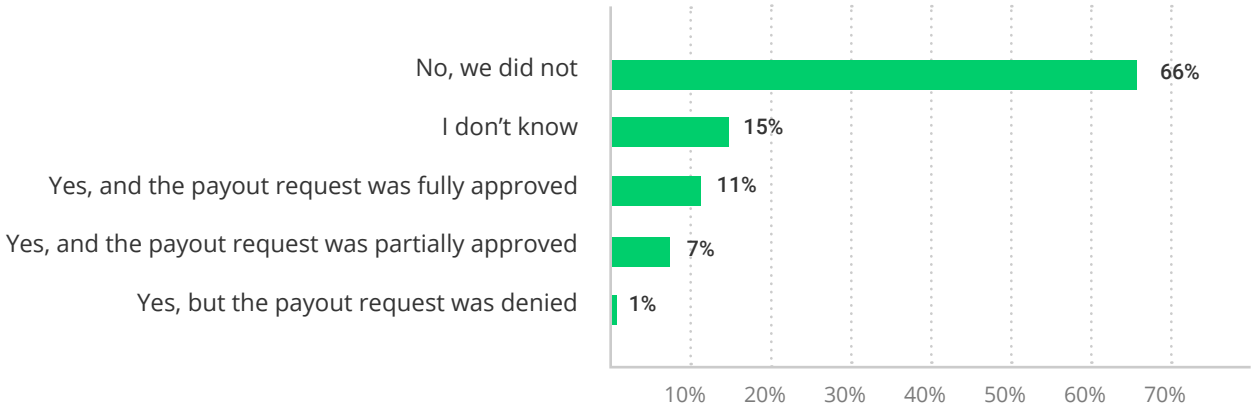
Dirk Schrader

VP of Security Research at Netwrix

POLICY CLAIMS

It's no wonder that the requirements for obtaining a cyber insurance policy have become stricter: The chance of a successful cyberattack – and, therefore, the chance of a payout request – is alarmingly high. Almost 1 in 5 (19%) insured organizations used their cyber insurance policy last year.

Did your organization use its cyber insurance policy in the last 12 months?



Two key forces driving 'baseline' security are insurance requirements and compliance regulations. Both change as technology and the threat landscape evolve, but insurance companies are more agile, adjusting their requirements faster and with greater attention to detail. As technology megatrends like quantum computing and AI open new attack vectors, we can expect to see new security controls required by the cyber insurance industry.

Ilia Sotnikov

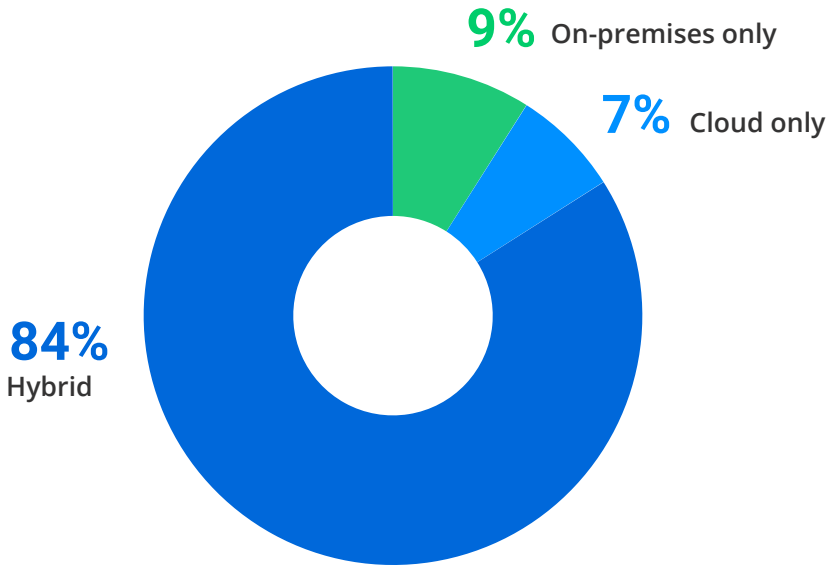
Security Strategist at Netwrix

APPENDIX. ADDITIONAL FINDINGS FOR THE ENTERPRISE SECTOR

CLOUD ADOPTION

Enterprises (over 1,000 employees) are moving to the cloud faster than smaller organizations. While on average, 74% of respondents say they have a hybrid infrastructure, this number is higher for the enterprise sector (84%). Subsequently, only 9% of large organizations are on premises only compared to 15% for the market average.

IT Architecture: Enterprises



IT PRIORITIES

The two main IT priorities are the same for organizations of all sizes: data security and network security. Automation of manual IT processes ranked third for the enterprise sector–almost half (49%) of respondents named it among their top priorities for 2024 compared to just fifth place for respondents overall.

Top IT priorities for the enterprise sector

Fully automated security solutions are often seen as a desirable goal. But what if that automation becomes compromised? Enterprises have to include these considerations in their risk management programs. While automation-related risks may require new mitigations, current controls like just-in-time access or access review process in place can help address these new risks.

Ilia Sotnikov

Security Strategist at Netwrix

For the IT and security departments, automation can offer benefits for a full range of tasks. First, it can help establish self-service for users without jeopardizing security, such as when users are granted local admin rights for their endpoints. Next, IT teams can seek to increase the automation of cloud and container management and improve log event analysis so that responses to detected incidents can be automated.

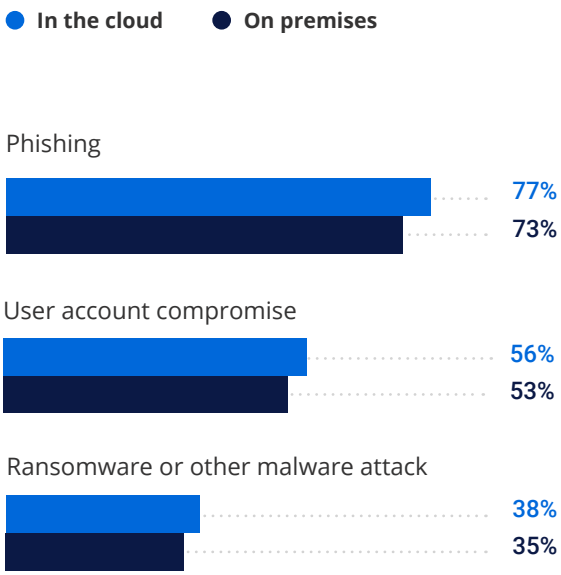
Dirk Schrader

VP of Security Research at Netwrix

SECURITY INCIDENTS

84% of organizations in the enterprise sector spotted a cyberattack within the last 12 months, compared to only 65% in 2023. Moreover, this rate is higher than the results among companies of all sizes in 2024: 79% of respondents say they detected an attack in their IT infrastructure.

Most common security incidents in the enterprise sector



The surge in the attack rates across organizations of all sizes, including the enterprise sector, may indicate that threat actors found AI automation extremely beneficial. With the introduction of AI, sending a massive number of phishing emails and probing systems and services for vulnerabilities is only a matter of orchestration on those platforms operated by cybercriminals. Constant pressure stresses the security teams and might lead to reduced and worn-out protection levels. To ease this burden, organizations should consider involving third-party investigators as a part of their incident response plan. It will help offload the internal security team when dealing with an ongoing attack.

Dirk Schrader

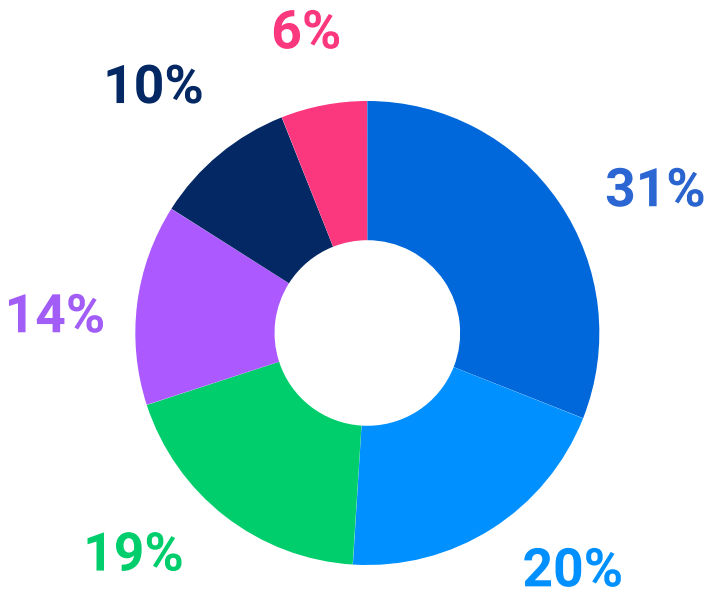
VP of Security Research at Netwrix

COST OF CYBERATTACKS

For 53% of large organizations, a cyberattack resulted in additional unexpected expenses to fix security gaps, compared to 45% among organizations overall. Each fifth enterprise faced compliance fines (22%) and a reduced competitive edge (21%). Moreover, 30% of enterprises estimated their financial damage from cyber threats to be at least $50,000, compared to just 17% among organizations overall.

Estimated financial damage due to cyber threats for large enterprises

- 0$
- $1 – $10,000
- $10,001 – $50,000
- $50,001 – $200,000
- $50,001 – $200,000
- $500,001 or more

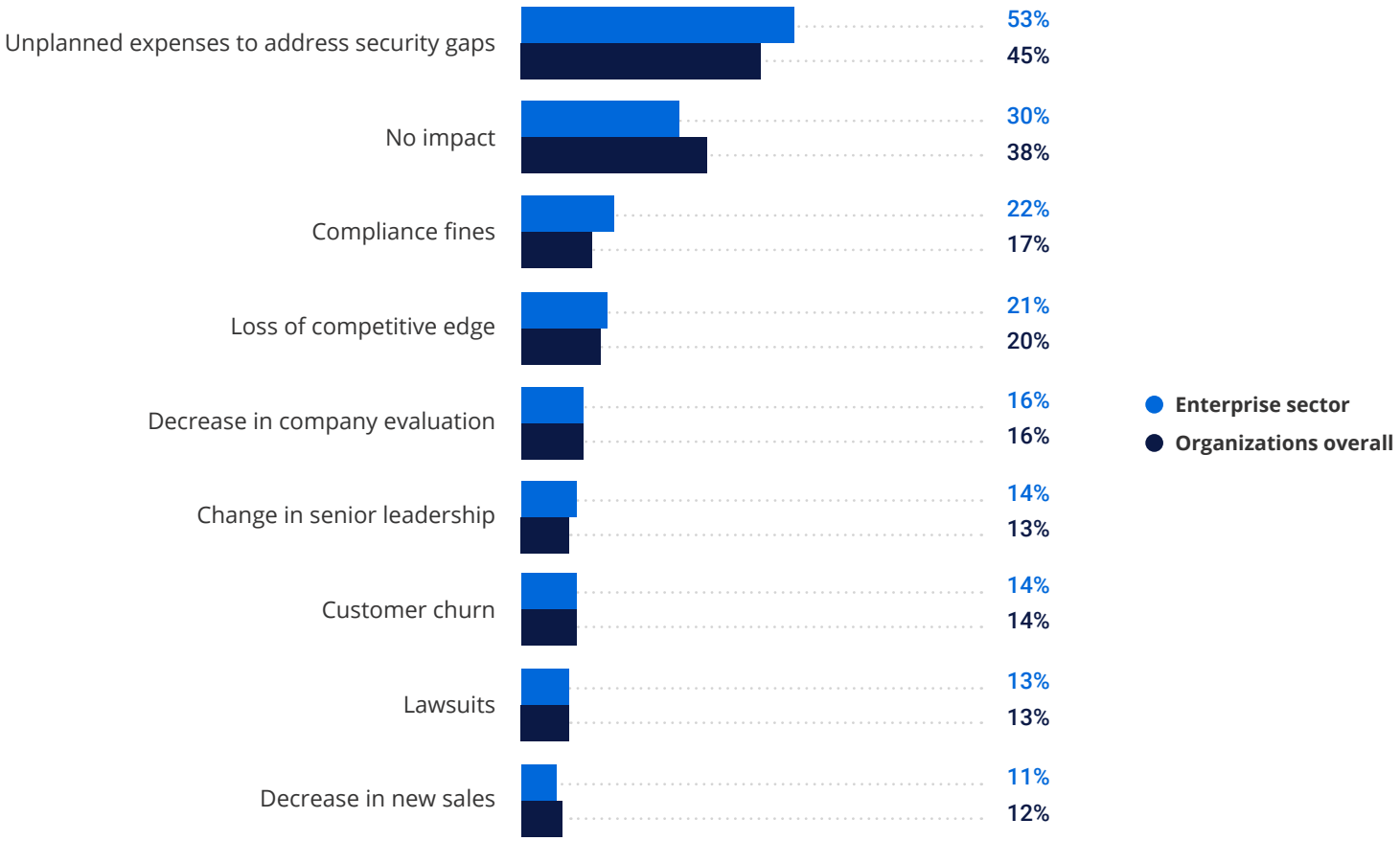


Mature security teams do not solely rely on preventative controls. They are investing in detection and remediation solutions as part of the defense-in-depth strategy, contributing to the growth in incident reports. Moreover, both the industry and the governments' expectations about security transparency are changing, increasing visibility into the real scale of the problem.

Ilia Sotnikov

Security Strategist at Netwrix

Cyberattack consequences for large enterprises



Typically, large enterprises have already implemented the basic security controls and thus must address more complex and costly issues in the aftermath of an attack. Where a smaller organization may have a quick fix available and can accept certain risks, enterprises must invest in the security team, process changes, and tooling to close even the smallest gaps exploited by the attacker.

Ilia Sotnikov

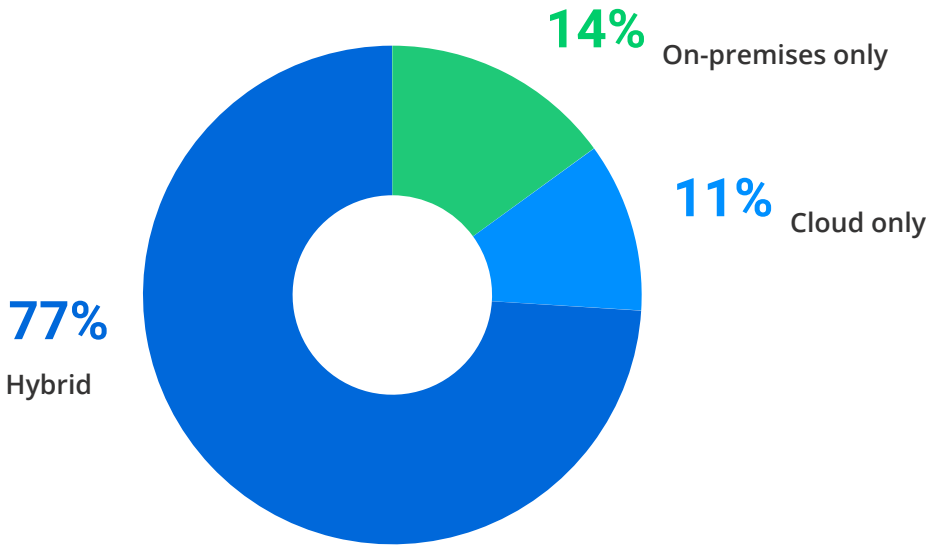
Security Strategist at Netwrix

MANAGED SERVICE PROVIDER (MSP) SECTOR

CLOUD ADOPTION

Managed service providers adopt cloud technologies at a pace similar to that of the rest of the market. About 3 in 4 MSPs have a hybrid IT architecture, and 11% are cloud-only.

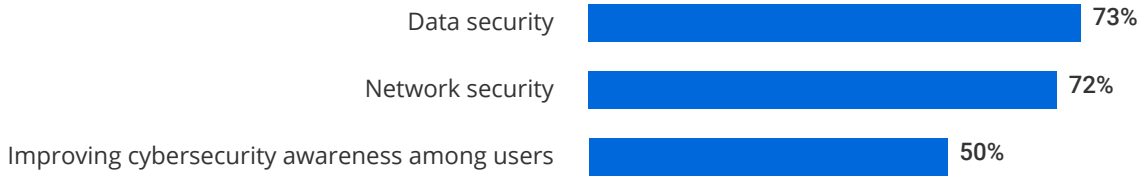
IT architecture of MSPs



IT PRIORITIES

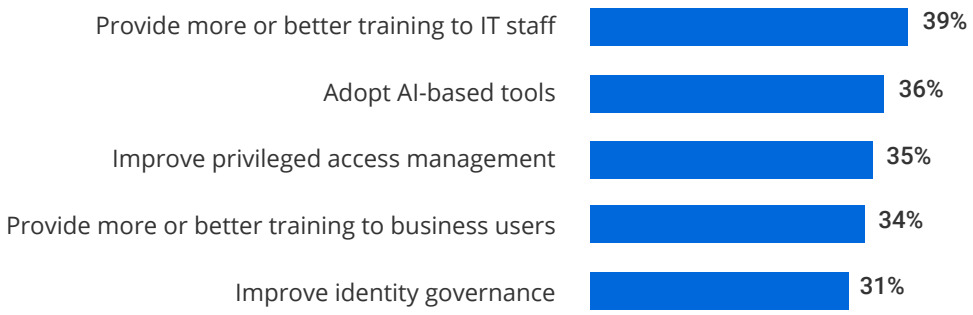
Like in 2023, the top IT priorities for the MSP sector are data security and network security, both of which were named by 7 in 10 MSPs.

Top organizational IT priorities for MSPs



We also asked our respondents what enhancements they would implement if they could choose how to improve their organization's security posture. The most desirable changes lie in the training area for IT staff and regular users. Surprisingly, implementing AI-based tools ranked second, while in the other industries, it was in seventh place.

Cybersecurity measures that IT pros working for MSPs would prioritize



AI technology promises the most desirable outcome for every MSP: Augment of the human talent resulting in better service at a lower cost to more clients. While operating within numerous IT environments, one of the most time-consuming tasks is the analysis of incoming signals. Delegating the navigation of benign notifications, false positive alerts, and actual attack patterns to an AI tool sounds promising. Still, only time will show when this scenario becomes feasible.

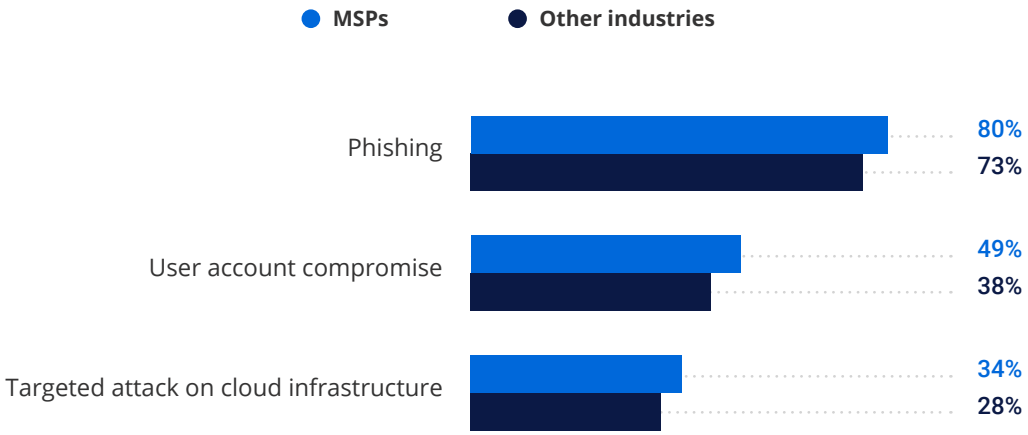
Dirk Schrader

VP of Security Research at Netwrix

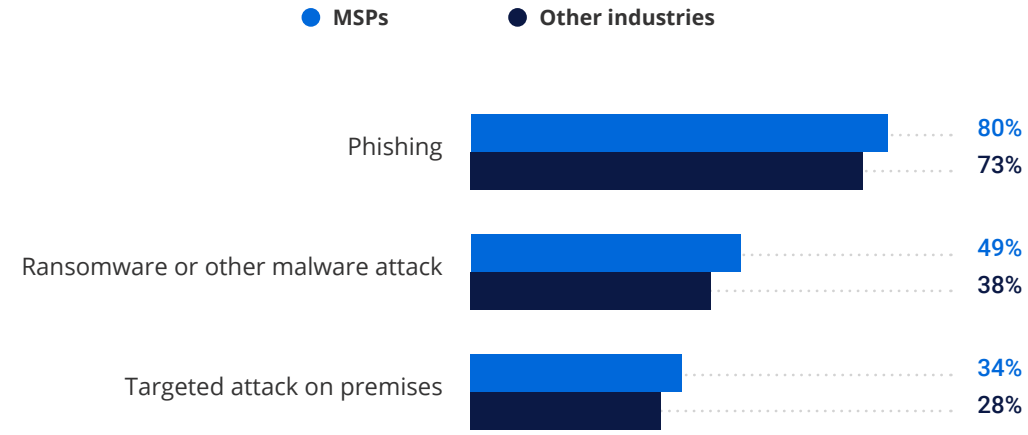
SECURITY INCIDENTS

76% of MSPs spotted a cyberattack on their infrastructure within the last 12 months, similar to the results among organizations overall (79%). For the MSP sector, each second security incident in the cloud was associated with user account compromise, while 46% of attacks on premises were ransomware or other malware attacks. In contrast, these types of attacks were less common among other industries.

Most common security incidents in the cloud for MSPs



Most common security incidents on premises for MSPs



MSPs largely rely on software-as-a-service (SaaS), platform-as-a-service (PaaS), and infrastructure-as-a-service (IaaS) solutions. These are usually accessible to both MSPs and their clients, significantly limiting the implementation of network-based restrictions like IP address filters. As a result, attackers target such cloud-based solutions because they might be easier to infiltrate, and one successful breach gives keys to many kingdoms.

Dirk Schrader

VP of Security Research at Netwrix

The service provider is a promising target for ransomware gangs. On one hand, MSPs can hardly afford downtime and would be more eager to have the operations back up and running, which increases the chances for ransom payout. On the other hand, breaching a service provider can be just a step toward the real target in a supply chain attack. MSPs should adequately assess the risks and rely on threat intelligence to make their security decisions.

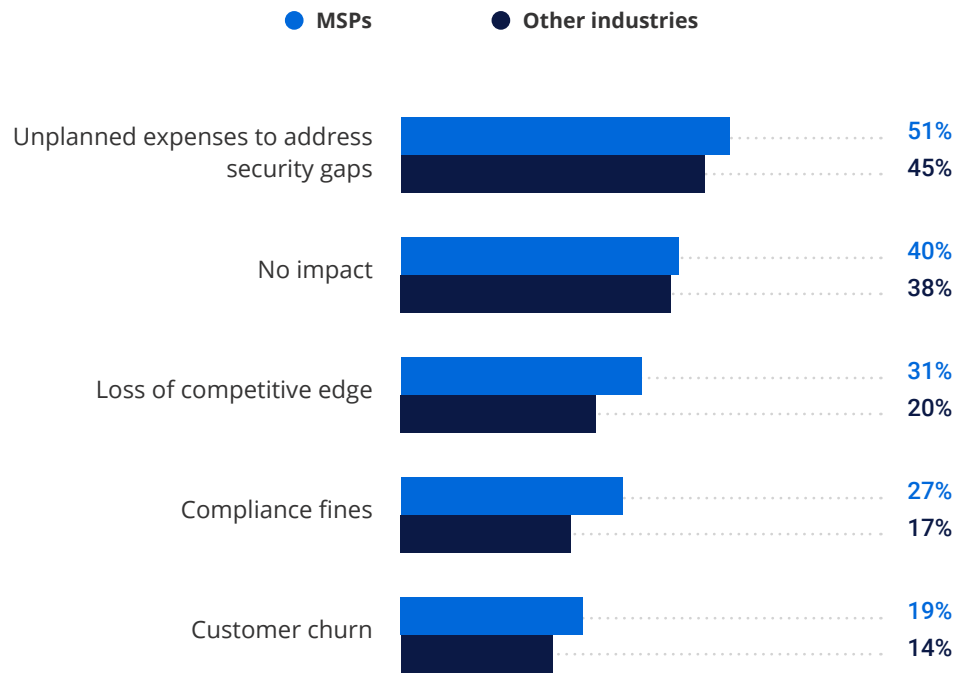
Ilia Sotnikov

Security Strategist at Netwrix

CYBERATTACK CONSEQUENCES

The survey reveals that the MSP sector suffers from cyberattack consequences more often than other industries. Among those that were attacked, every second MSP (51%) had to deal with unplanned expenses to fix the security gaps. Moreover, 31% experienced a loss of competitive edge, and 27% faced compliance fines compared to 20% and 17% across all other industries.

Cyberattack consequences for MSPs

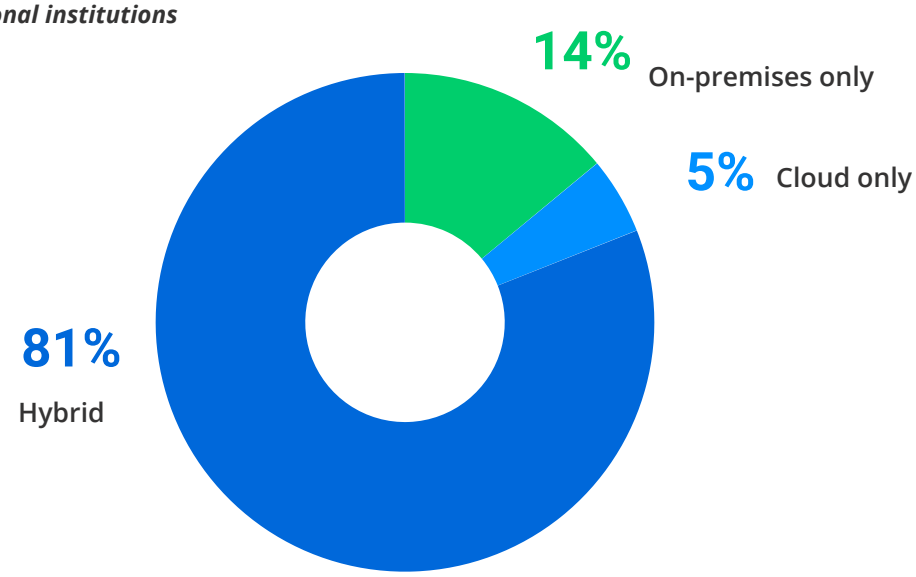


THE EDUCATION SECTOR

CLOUD ADOPTION

81% of educational institutions have a hybrid IT architecture compared to 74% across other industries. Among those 14% that are strictly on premises, 47% plan to adopt cloud technologies moving forward.

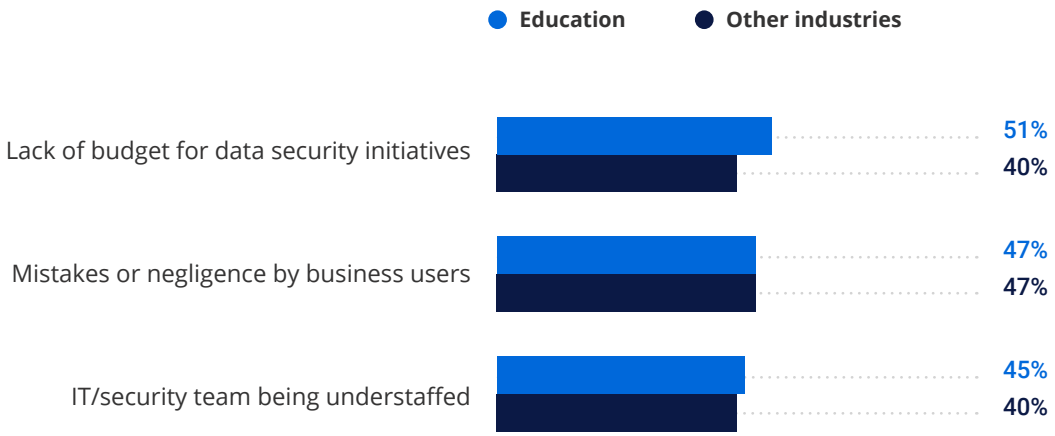
IT architecture of educational institutions



SECURITY CHALLENGES

Half of educational institutions (51%) name lack of budget as their biggest data security challenge, followed by users' mistakes and negligence.

Top data security challenges of educational institutions



Universities or school districts can have as many user accounts as some global multi-national businesses. While educational institutions may have the same complexity as large organizations, they typically lack matching budgets and resources to deal with their dynamic environments. It is crucial for the IT Security teams in the education sector to have processes and tools in place to govern the identities, audit their activity, and monitor for any abnormal or malicious behavior.

Ilia Sotnikov

Security Strategist at Netwrix

To enable research and collaboration, while staying on budget, educational institutions often provide a variety of shared devices and systems exposed to the internet — creating a massive attack surface. To mitigate risk, it is crucial to enforce strong password policies that prevent the use of weak and compromised passwords, implement multifactor authentication (MFA), and adhere to the least privilege principle.

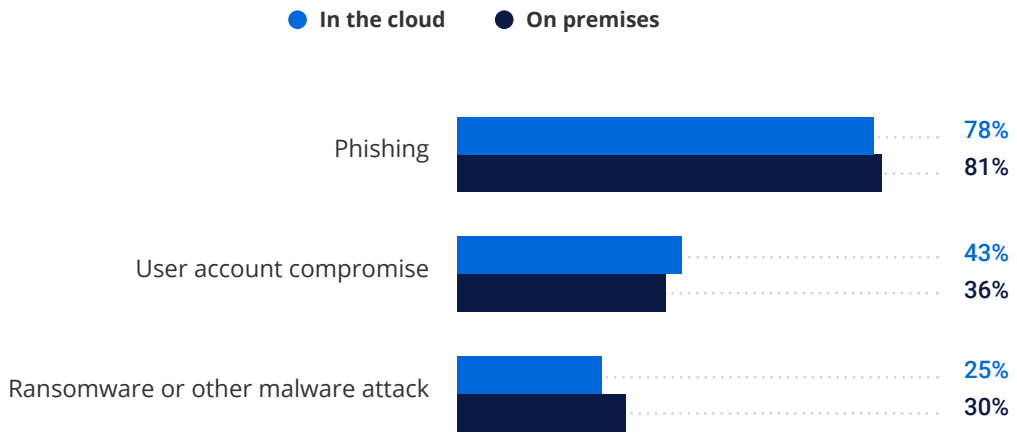
Dirk Schrader

VP of Security Research at Netwrix

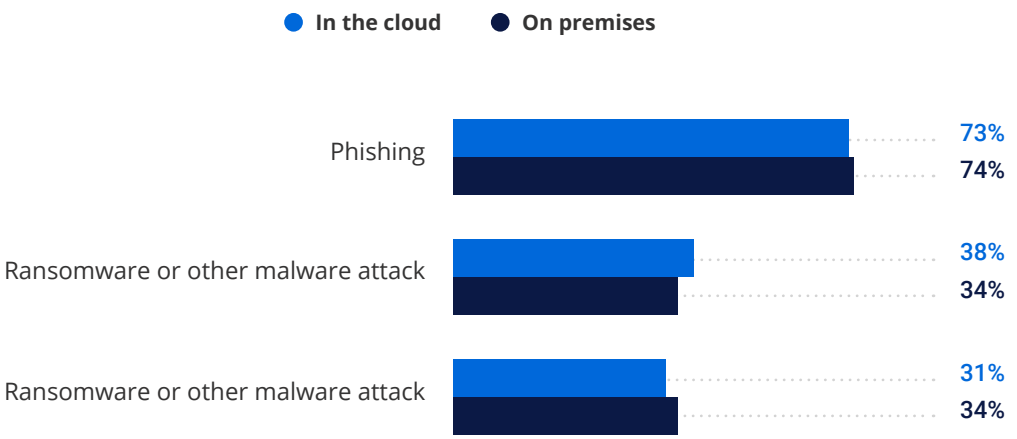
SECURITY INCIDENTS

77% of organizations in the education sector spotted a cyberattack on their infrastructure within the last 12 months, up from 69% in 2023. The most common attack vectors were similar to those among other industries: Phishing, user account compromise, and ransomware or other malware attacks.

Most common security incidents in the education sector



Most common security incidents across other industries



Many cloud services are given to the educational institutions at a discounted rate. Naturally, it leads to more frequent usage of such services. Default security settings combined with a high turnover of cloud identities in use results in a larger attack surface and, therefore, in more frequent attacks in the cloud compared with other industries surveyed.

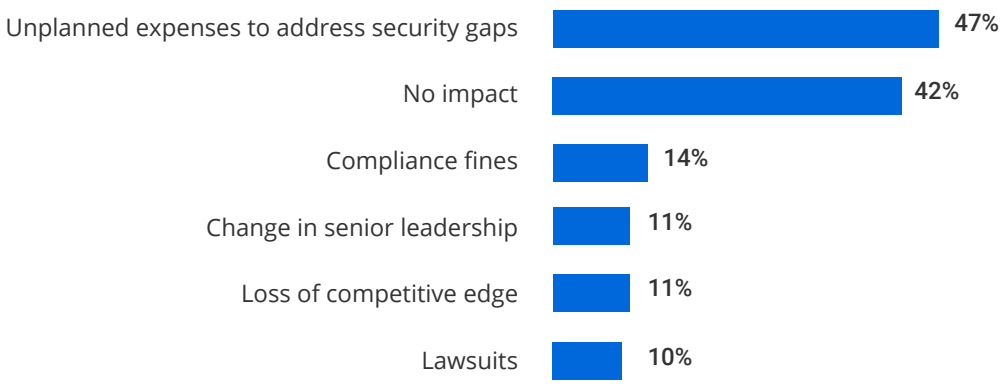
Dirk Schrader

VP of Security Research at Netwrix

CYBERATTACK CONSEQUENCES

Almost half (47%)of educational organizations faced unplanned expenses to fix security gaps because of a security incident. Moreover, 1 in 7 of those organizations incurred compliance fines, and each tenth reported changes in senior leadership and lawsuits.

Cyberattack consequences for the education sector



An incident can reveal security gaps such as excessive admin privileges, dormant accounts, weak or unchanged passwords, default passwords or configurations, and unpatched systems due to negligence or lack of knowledge. Fixing a gap might not immediately require spending additional money but will definitely require time from the IT security team. In other words, addressing the root cause of a security incident.

Dirk Schrader

VP of Security Research at Netwrix

In the aftermath of a breach, organizations must prioritize remediation steps to reduce risks moving forward. For example, the immediate response may include patching software on the most critical servers and adding a manual review step on certain operations. Longer-term remediation may have to wait for the next budget cycle and require additional software, services engagement, or headcount.

Ilia Sotnikov

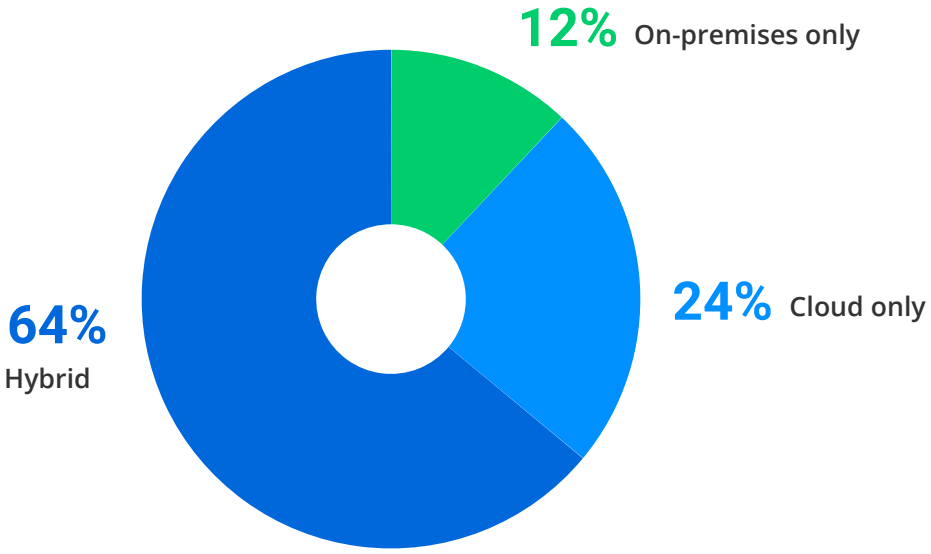
Security Strategist at Netwrix

THE HEALTHCARE SECTOR

CLOUD ADOPTION

Almost one-quarter (24%) of healthcare organizations are fully cloud-based, compared to only 11% in other industries. Moreover, while 74% of respondents overall have a hybrid infrastructure, this number is lower for the healthcare sector (64%).

IT architecture: Healthcare



The effort and cost of managing an on-premises infrastructure are higher in the healthcare sector, due in part to stringent regulatory standards around the handling and storage of patient and research data. In order to focus on their core healthcare mission, these organizations often offload significant parts of the security and compliance burden to software-as-a-service (SaaS) and infrastructure-as-a-service (IaaS) providers, which drives higher cloud adoption rates in this sector.

Ilia Sotnikov

Security Strategist at Netwrix

IT PRIORITIES

The two main IT priorities are the same for organizations across all sectors: data security and network security. Automation of manual IT processes ranked third for the healthcare sector, compared to just fifth place for respondents overall. Indeed, nearly half (46%) of healthcare organizations respondents picked it as one of their top priorities for 2024.

Top IT Priorities: Healthcare

Healthcare organizations traditionally deal with many processes that require manual input of information like treatment protocols, administered drugs, procedures performed — basically, everything that happens to a patient. Automating these processes saves the valuable time of healthcare professionals, so it's no wonder that automation is a high priority for this sector.

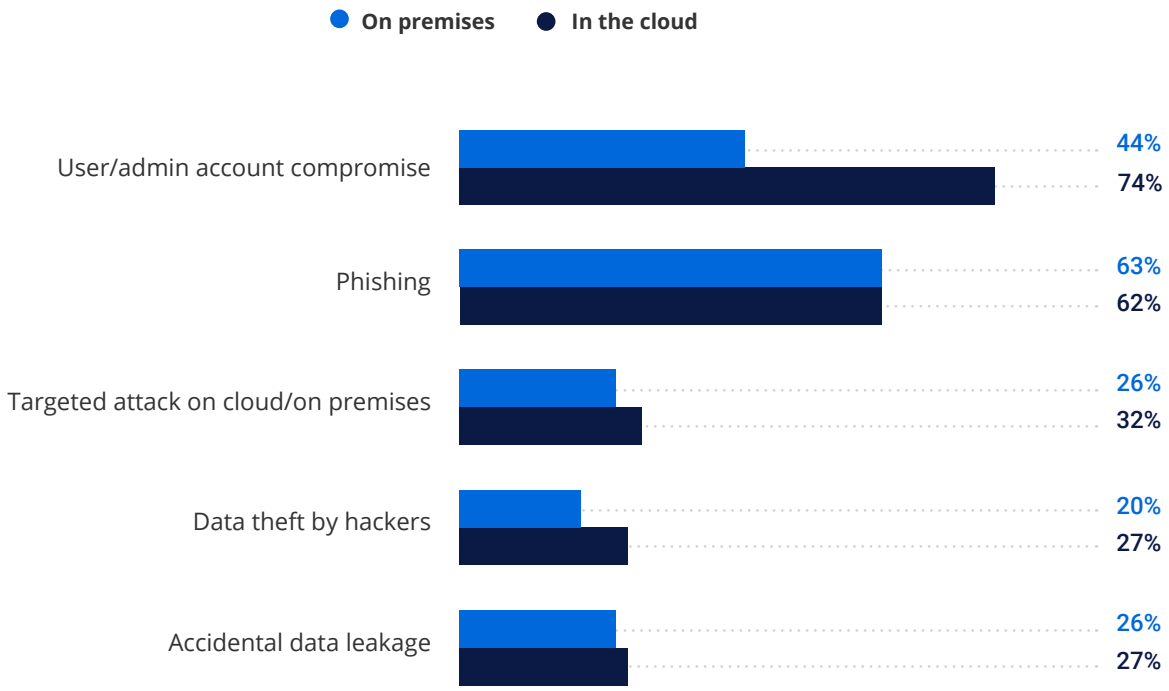
Dirk Schrader

VP of Security Research at Netwrix

SECURITY INCIDENTS

84% of organizations in the healthcare sector spotted a cyberattack within the last 12 months. Phishing was the most common type of incident experienced on premises, similar to other industries. Account compromise topped the list for cloud attacks: 74% of healthcare organizations that spotted a cyberattack reported user or admin account compromise.

Most Common Security Incidents: Healthcare



Healthcare workers regularly communicate with many people they do not know — patients, laboratory assistants, external auditors and more — so properly vetting every message is a huge burden. Plus, they do not realize how critical it is to be cautious, since security awareness training often takes a back seat to the urgent work of taking care of patients. Combined, these factors can lead to a higher rate of security incidents.

Dirk Schrader

VP of Security Research at Netwrix

Protected health information (PHI) is one of the most expensive types of data sold on darknet forums, which makes healthcare organizations a top target for cybercriminals. A core defense strategy is to minimize standing privileges by using a privileged access management (PAM) solution. Another is to implement identity threat detection and response (IDTR) tools to quickly block malicious actors using compromised credentials.

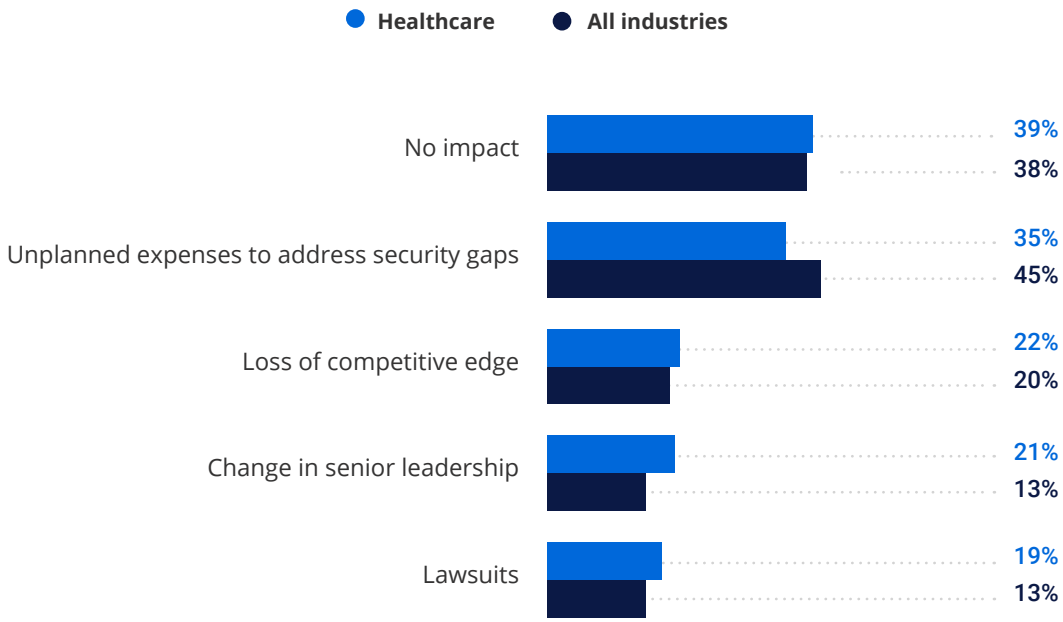
Ilia Sotnikov

Security Strategist at Netwrix

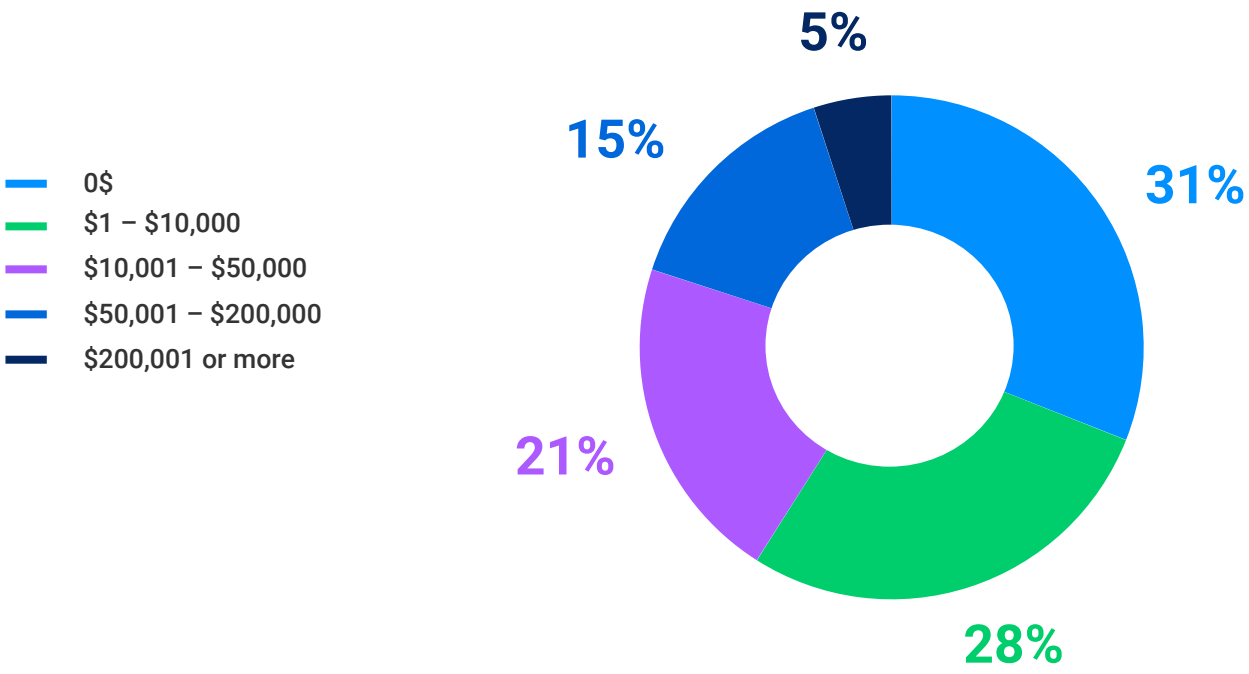
COST OF CYBERATTACKS

A cyberattack resulted in financial damage for 69% of healthcare organizations, compared to 60% among other industries. One in five healthcare organizations that suffered an attack experienced a change in senior leadership (21%) or lawsuits (19%) as a result, compared to 13% for each of these outcomes among all industries surveyed.

Cyberattack Consequences: Healthcare



Estimated Financial Damage due to Cyberattacks: Healthcare



ABOUT THE REPORT

The report is brought to you by Netwrix Research Lab, which conducts industry surveys among IT pros worldwide to discover important changes and trends. For more reports, please visit www.netwrix.com/research

ABOUT NETWRIX

Netwrix champions cybersecurity to ensure a brighter digital future for any organization. Netwrix's innovative solutions safeguard data, identities, and infrastructure reducing both the risk and impact of a breach for more than 13,500 organizations across 100+ countries. Netwrix empowers security professionals to face digital threats with confidence by enabling them to identify and protect sensitive data as well as to detect, respond to, and recover from attacks.

For more information, visit www.netwrix.com

Corporate Headquarters:
6160 Warren Parkway, Suite 100, Frisco, TX, US 75034
Phone: 1-949-407-5125 **Toll-free:** 888-638-9749 **EMEA:** +44 (0) 203-588-3023
www.netwrix.com/social