netwrix

2023 Hybrid Security Trends

CONTENTS

EXECUTIVE SUMMARY

Cloud adoption is in full swing, with 81% of organizations worldwide now using at least one cloud environment. To keep up with the evolution of IT security both on premises and in the cloud, Netwrix Research Lab surveyed 1,610 IT professionals from 106 countries via an online questionnaire in February 2023, and compared the results to its Cloud Data Security Reports from 2022, 2020 and 2019 and its IT Trends Report from 2020. The resulting report will help organizations concentrate their security efforts on what really matters. Key findings include the following:

IT ARCHITECTURE

The cloud is an integral part of the IT infrastructure for most organizations: 73% of them have a hybrid IT environment. Moreover, on average, organizations report that 44% of their workloads are already in the cloud.

SECURITY CHALLENGES

The top security concern for on-premises infrastructures is understaffed IT teams, while for cloud environments, it is lack of budget.

SECURITY INCIDENTS

68% of organizations suffered a cyberattack within the last 12 months; phishing was the most common attack vector. On-premises infrastructures suffered more cyberattacks than the cloud. The starkest difference was for ransomware and other malware attacks, which were reported by nearly twice as many respondents for on-premises environments (37%) as for the cloud (19%).

DATA BREACH CONSEQUENCES

53% of organizations that suffered a data breach faced financial consequences as a result. About 1 in 10 reported other serious consequences, such as loss of competitive edge, decreased sales or customer churn.

SECURITY MEASURES IN PLACE

On premises, the three most common security measures being used are backups, password management and multifactor authentication (MFA); for the cloud, MFA topped the list, followed by backups and encryption.

PLANNED SECURITY MEASURES

Identity governance topped the list of measures that organizations plan to implement to improve cybersecurity, both on premises and in the cloud.

IT PRIORITIES

The main areas of concern for 2023 have stayed the same since 2019: data security, network security and cybersecurity training. Two areas that gained ground were cloud adoption and supporting existing cloud infrastructures.

CYBER INSURANCE

59% of organizations have a cyber insurance policy or plan to purchase one within 12 months. 28% organizations that have cyber insurance changed their security approach in order to reduce their premium — and 22% had to improve their security posture to even be eligible for the policy.

NETWRIX RESEARCH LAB EXPERTS

DMITRY SOTNIKOV

Vice President of Product Management at Netwrix

Dmitry has more than two decades of experience in enterprise IT software and cloud computing. His team is in charge of product management and roadmaps across all sixteen products in the Netwrix portfolio.

Prior to joining Netwrix, Dmitry held executive positions at companies such as 42Crunch, WSO2, Jelastic and Quest Software.

Dmitry has master's degrees in Computer Science and in Economics and Management. He is a member of the Advisory Board at the University of California, Riverside Extension. He has also earned 11 Microsoft MVP awards.

DIRK SCHRADER

Vice President of Security Research 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.

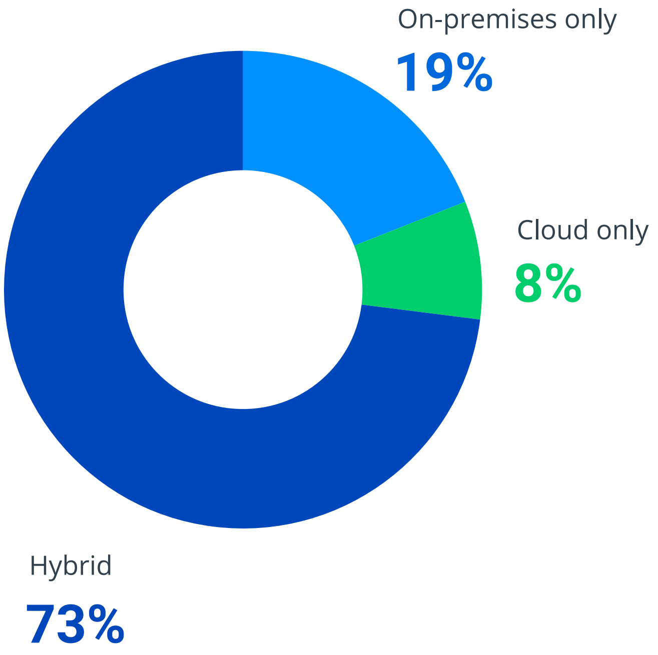
Along with general security research and vulnerability discovery, Dirk is keen on industry-specific focused research for verticals like healthcare, energy and finance. He has reported hundreds of vulnerable medical devices to authorities and health providers around the globe.

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

IT ARCHITECTURE

In 2023, with remote and hybrid work now commonplace, it is no surprise that the cloud is an integral part of the IT infrastructure for most organizations.

Organization's IT architecture



69%

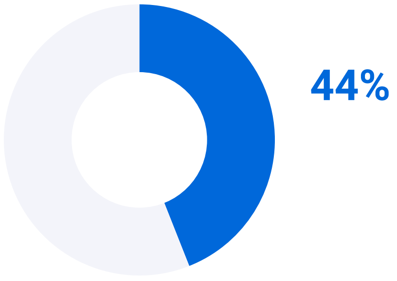
of those who currently stays on-premises only, plan to adopt cloud technologies.

37%

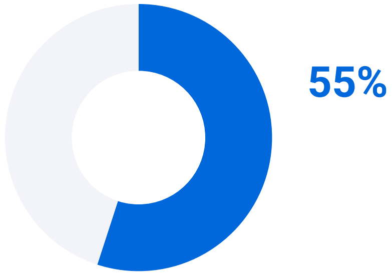
of those who currently stays on-premises only, plan to adopt cloud technologies within the next 12 months.

On average, organizations report that 44% of their workloads are already in the cloud, and they expect that share to increase to 55% by the beginning of 2024.

What percentage of your organization workloads are already in the cloud?



What percentage of your organization workloads are planned to be in the cloud 12 months from now?



Cloud adoption progressed more slowly than our respondents anticipated in past year: The average share of workloads in the cloud inched up from 41% to 44%, not to 54% as the 2022 survey respondents expected.

Indeed, in 2022, the main factor slowing cloud adoption, named by 41% of organizations, was integration with the existing IT environment, and only 11% of respondents said they were moving to the cloud as quickly as they needed.

The slower pace of cloud adoption proves that organizations are addressing this challenge with diligence. Moving to the cloud is not a copy-and-paste thing — it requires careful planning, expectation management, and sufficient resources for process testing and re-engineering. Forced attempts to accelerate cloud migration can lead to significant expenses overrun and can even require costly architecture redesign if issues are found later in the process. Accordingly, it is vital to use security tools that help cover both on-prem and cloud systems to avoid security incidents when the IT environment is in its most vulnerable state: the state of change.

Dirk Schrader

VP of Security Research at Netwrix

IT projects generally tend to take longer than expected, and migration to the cloud is no exception. The devil is in the details: Companies have accumulated significant on-prem infrastructure and switching to the cloud while maintaining business operations is not easy. Software as a service (SaaS) is typically the most cost-effective approach, but vendors rarely offer SaaS solutions that are fully equivalent to their on-prem products. Migration paths are not simple either; business applications may be deeply integrated with other systems, making migration costly and disruptive. A lift-and-shift approach might appear to be the easiest because on-prem products can be run on virtual machines in a cloud datacenter — but it still requires migration and can lead to increased hosting costs. As a result, companies quickly get into hybrid mode with cloud-native applications like email and CRM but still must maintain on-prem infrastructure for tools that are hard or costly to migrate.

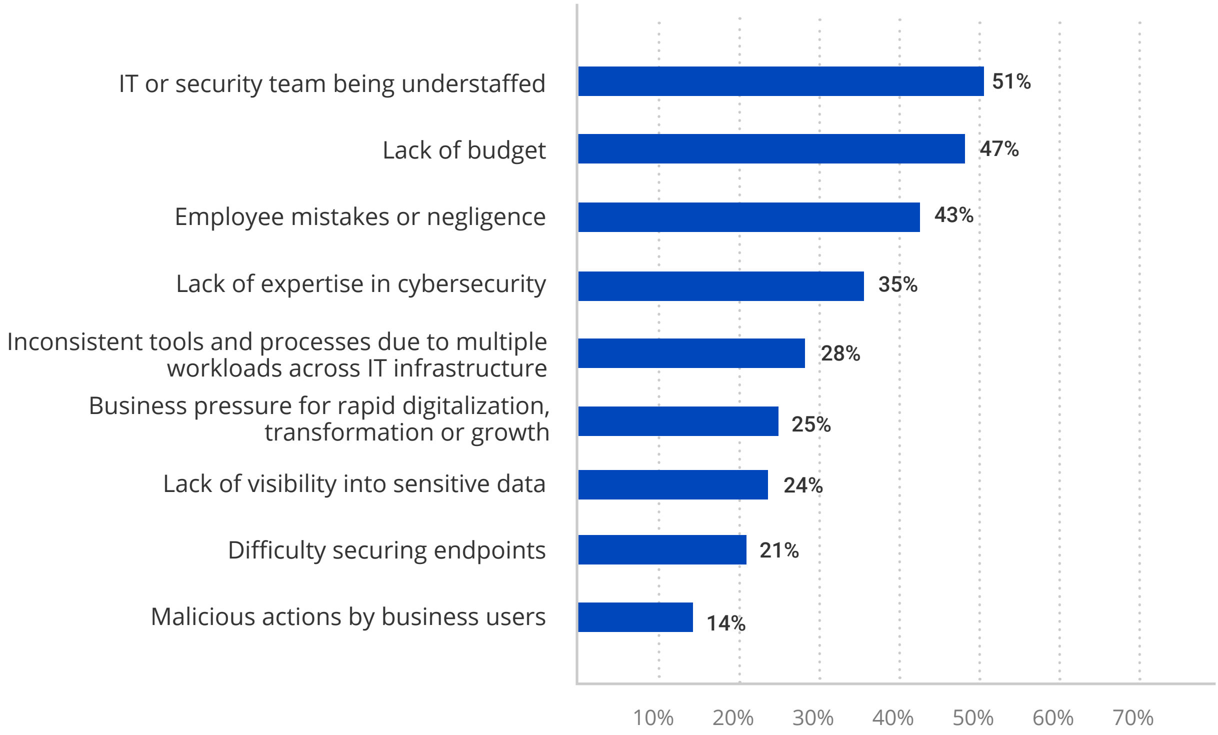
Dmitry Sotnikov

VP of Product Management at Netwrix

SECURITY CHALLENGES

Before digging into current threat landscape, we asked our respondents to share their thoughts about what hinders their efforts to ensure the security of sensitive data that their organizations store. Understaffing of the IT team topped the list, followed by lack of budget and employee mistakes.

What are the biggest challenges you face while trying to ensure data security?



Employee errors and negligence are a big area of concern as well. Along with cybersecurity training, business users need help from technology. In particular, system hardening, change control, and identity and access management (IAM) can help prevent improper exposure of sensitive data and other security incidents.

Dirk Schrader

VP of Security Research at Netwrix

When an IT team understaffed, every working minute is critical. The resulting stress and long hours can lead to fatigue and possibly mistakes, which are never a good thing in the world of cybersecurity. One way to address this challenge is to automate routine tasks like access management and Active Directory group management. Other measures include using mature security products that produce fewer false positive alerts and relying on a select group of trusted vendors that have an extensive portfolio and a unified support team. Smaller organizations may want to partner with a managed service providers (MSP) to bridge the gaps.

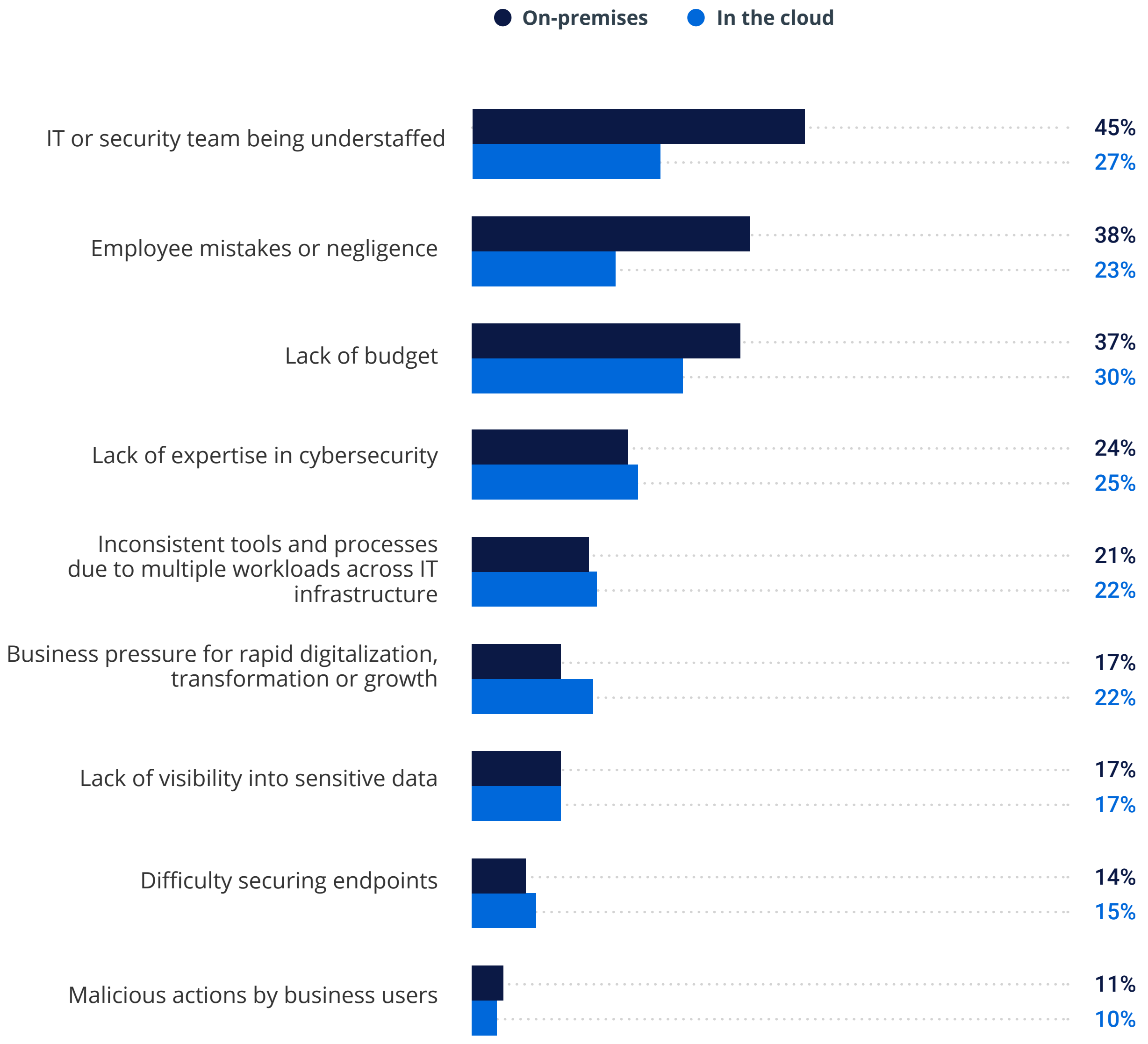
Dmitry Sotnikov

VP of Product Management at Netwrix

IN THE CLOUD VS ON-PREMISES

The chart above shows the security challenges facing organizations overall. When we asked the respondents about their top challenges in each of the two parts of their IT infrastructure, clear differences came to light. In particular, the top concern for cloud infrastructures is not understaffed IT teams but lack of budget, and mistakes by employees are less of a security concern in the cloud than on premises.

What are the biggest challenges you face while trying to ensure data security?



> **Moving to the cloud often means that IT tasks like physical security, networking and patching get outsourced to the cloud provider, so it's no surprise that understaffing on internal IT teams is less of a security concern for cloud-based workloads. In general, SaaS solutions can offload more IT tasks than platform-as-a-service (PaaS) or infrastructure-as-a-service (IaaS) technologies.**

Dmitry Sotnikov

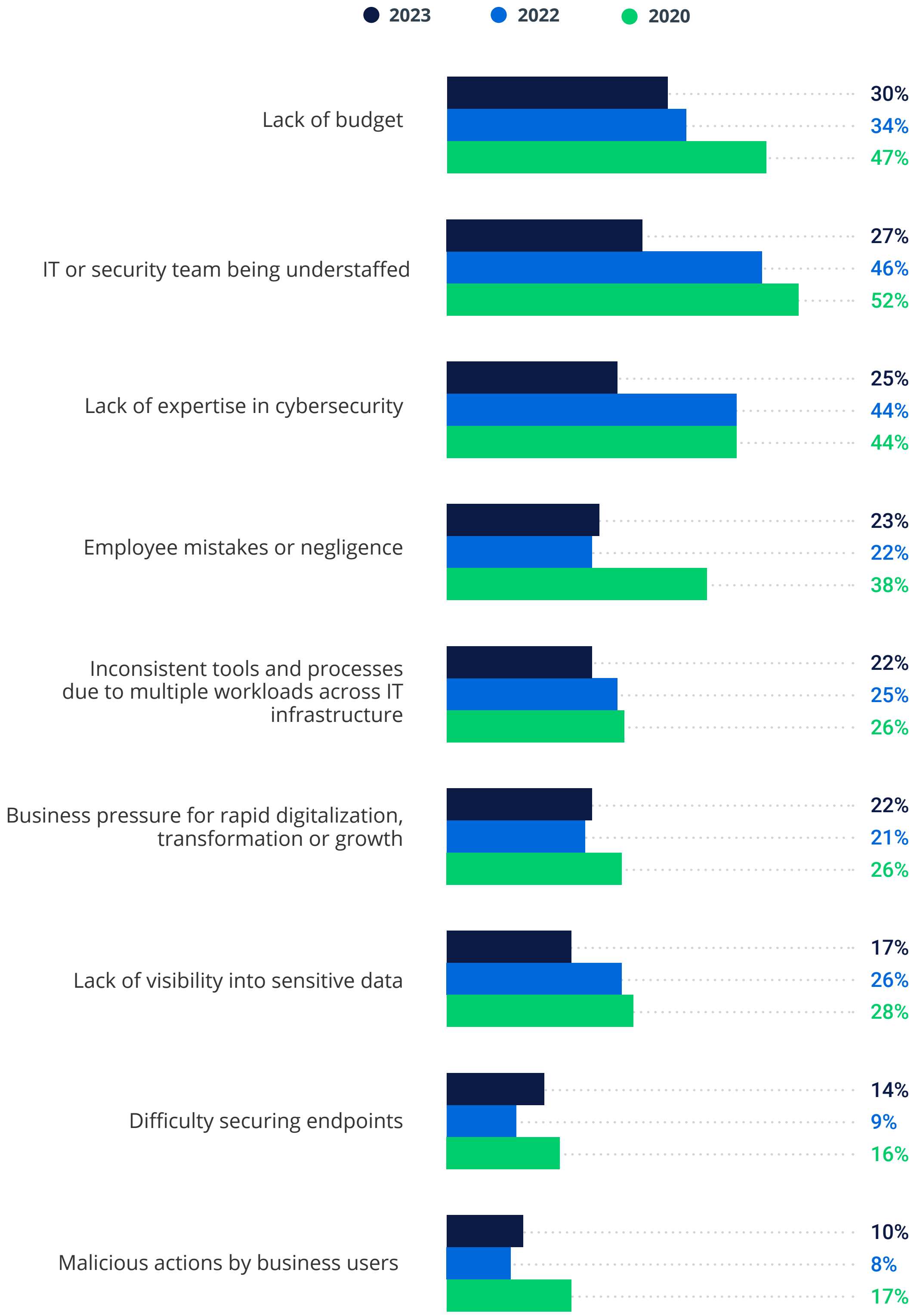
VP of Product Management at Netwrix

Employee mistakes or negligence is the main concern for fully cloud-based organizations

Lack of budget is the main concern for on-premises only organizations

SHIFT IN CLOUD SECURITY CHALLENGES OVER TIME

What are the biggest challenges you face while trying to ensure data security in the cloud?



We compared the results of this year's survey with those from 2022 and 2020. Interestingly, the top areas of concern remained the same — insufficient IT staff, budget and cybersecurity expertise — far fewer respondents now worry about those challenges.

In 2022, more than half (51%) of respondents named security improvement as a primary goal in cloud adoption. This year's survey results show that they achieved that goal — IT teams are more confident about cloud security because they have improved their cloud skills and learned how to use the technologies more securely.

Dmitry Sotnikov

VP of Product Management at Netwrix

Nevertheless, inconsistency in coverage of cloud and on-premises estates still poses an issue. To avoid security gaps and ensure clear visibility, it is crucial to have tools that can monitor the entire IT environment. For example, it's important to use an IAM product that can integrate cloud applications into provisioning, deprovisioning workflows to unify cloud and on-prem access management.

Dirk Schrader

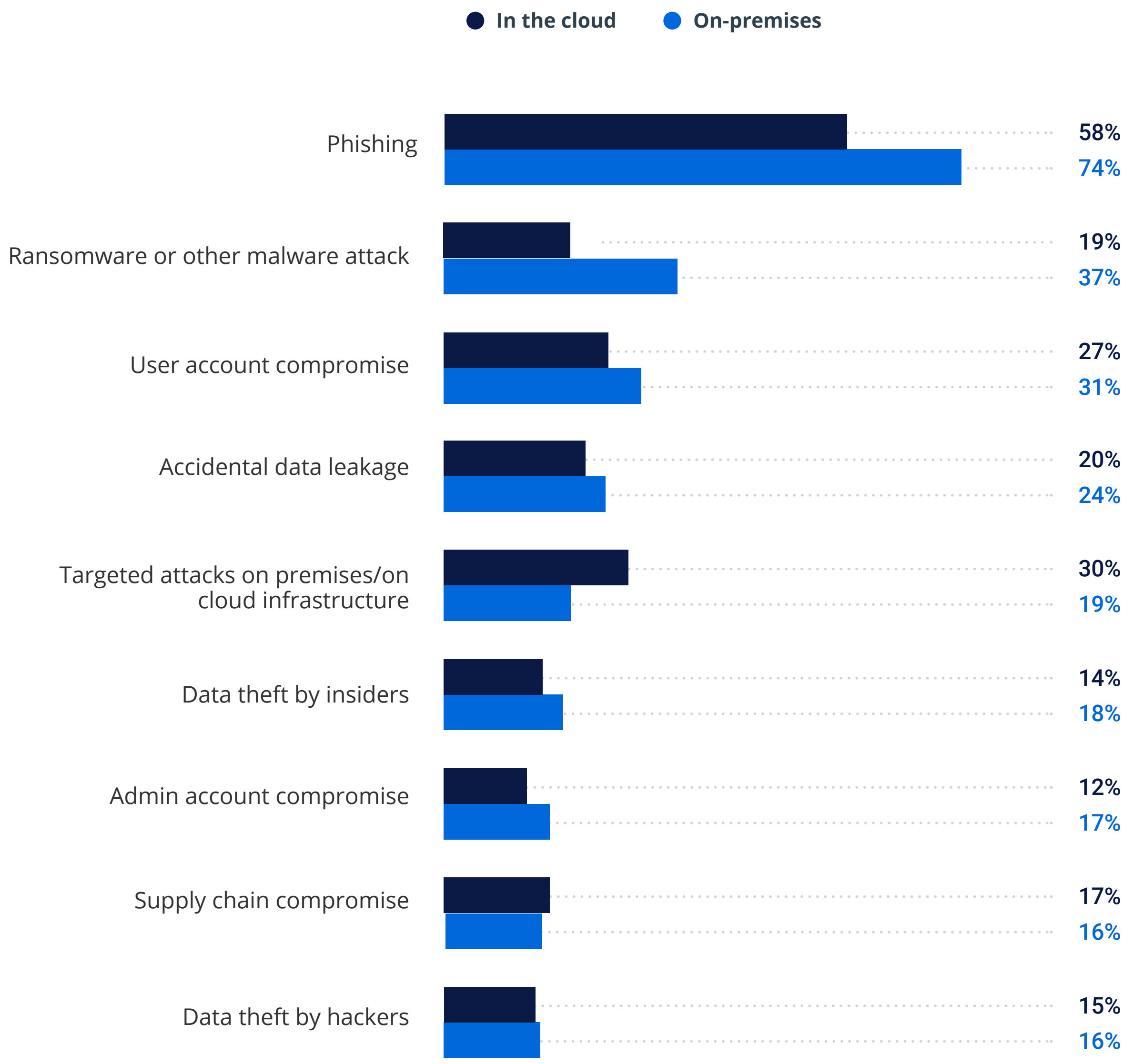
VP of Security Research at Netwrix

SECURITY INCIDENTS

IN THE CLOUD VS ON PREMISES

68% of organizations suffered a cyberattack within the last 12 months. Security professionals know that it's impossible to achieve full cybersecurity, which means that the remaining 32% had a very lucky year — or just haven't discovered the incident yet. We asked those who experienced cyberattacks to provide details on what happened. The results show that on-premises infrastructure suffers more cyberattacks than the cloud. The starkest difference was for ransomware and other malware attacks, which were reported by nearly twice as many respondents for on-premises environments (37%) as for the cloud (19%).

Most common security incidents



On-prem environments are more vulnerable to these types of attacks than SaaS systems as they often have sprawling privileges on the infrastructure level. For example, users might have administrative rights on their computers, privileged domain and server accounts, database accounts, and so on. Unless a zero-standing privilege approach is implemented, any excessive rights enable ransomware to compromise an endpoint and quickly spread across the on-prem systems.

Dmitry Sotnikov
VP of Product Management
at Netwrix

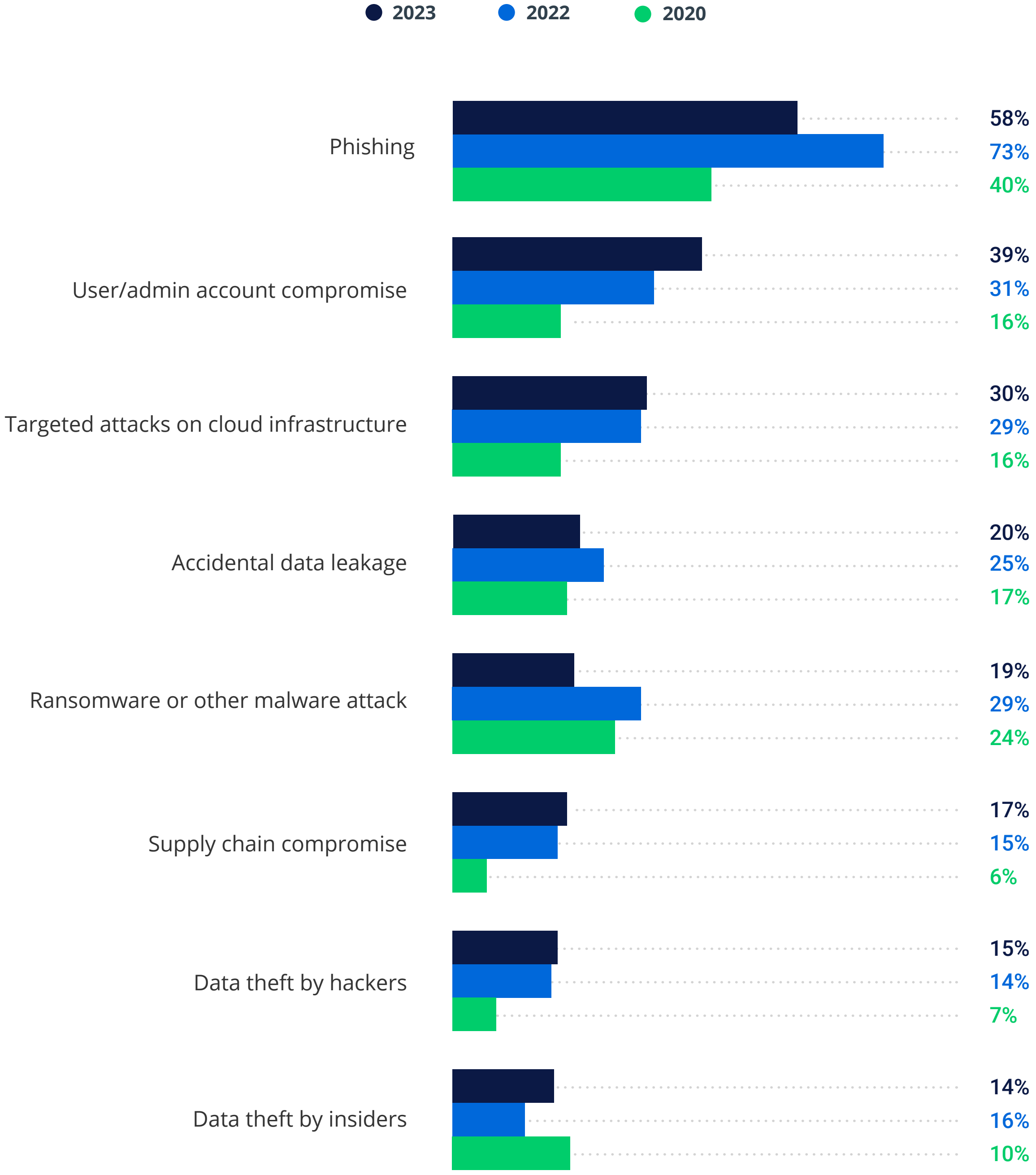
Phishing remains still the most common attack vector. Phishing emails used to be easy to spot, thanks to grammar and spelling mistakes and obviously incorrect graphics. But the advent of AI tools like ChatGPT will make it easy for threat actors to quickly create well-formed messages, including spear-phishing messages that target specific individuals, that are likely to fool more recipients into clicking on malicious links or opening infected attachments. Similarly, they will be able to easily craft convincing webpages that are more likely to lure targets into providing their credentials or other sensitive data. To be prepared for such attacks, organizations update their user awareness training and pay closer attention to securing user identities. In particular, it is essential to implement a zero standing privilege approach in which privileges exist only when they are needed.

Dirk Schrader
VP of Security Research
at Netwrix

SECURITY INCIDENTS IN THE CLOUD

We also compared this year's results about security incidents in the cloud to those from 2020 and 2022. While phishing remains the most common incident type, the other incidents have shifted positions. User and admin account compromise is now in second place, with 39% of respondents experiencing it in 2023 compared to 31% in 2022 and just 16% in 2020.

Most common security incidents in the cloud



Spear-phishing campaigns target high-value accounts. With the power of AI-based social engineering now readily available, attackers are well positioned to compromise privileged accounts and gain control of Active Directory infrastructures. As a result, we see an increase in successful credential abuse even though fewer organizations are reporting phishing attacks.

Dirk Schrader

VP of Security Research at Netwrix

Attackers seek to compromise administrative accounts because they can use them to spread laterally to other systems. Gaining privileged access to business-critical applications and infrastructure, such as enterprise resource planning (ERP) and customer relationship management (CRM) systems, gives adversaries the ability to destroy sensitive data or hold it hostage for ransom. Accordingly, it is crucial to implement a zero standing privilege approach that ensures administrative accounts exist only as long as needed to complete a specific task, minimizing the risk of an attacker gaining privileged access.

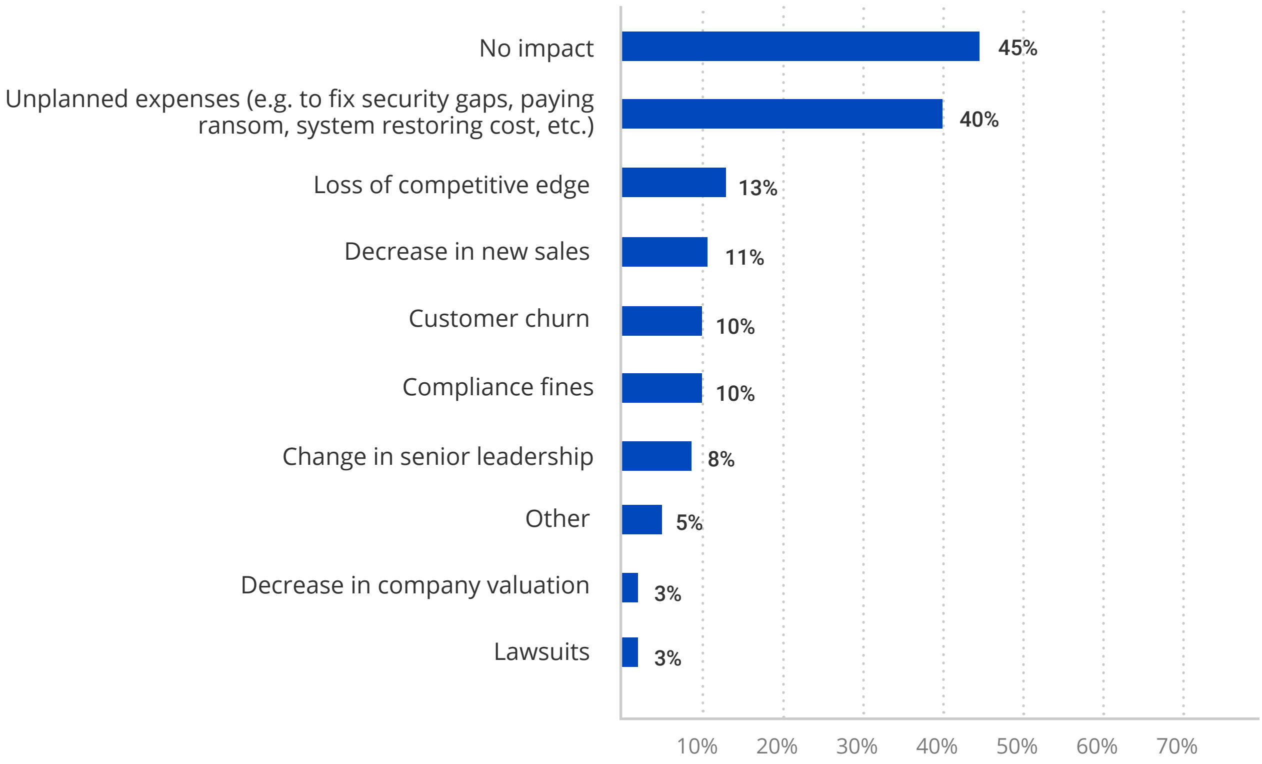
Dmitry Sotnikov

VP of Product Management at Netwrix

DATA BREACH CONSEQUENCES

Some cyberattacks have dire consequences, including freezing operations so long that the organization goes out of business, but most organizations survive the cyberattacks they experience. Indeed, 45% of respondents who suffered a cyberattack say it had no significant impact on their organization. However, 40% faced unplanned expenses, and about 1 in 10 reported other serious consequences, such as loss of competitive edge, decreased sales or customer churn.

Data breach consequences

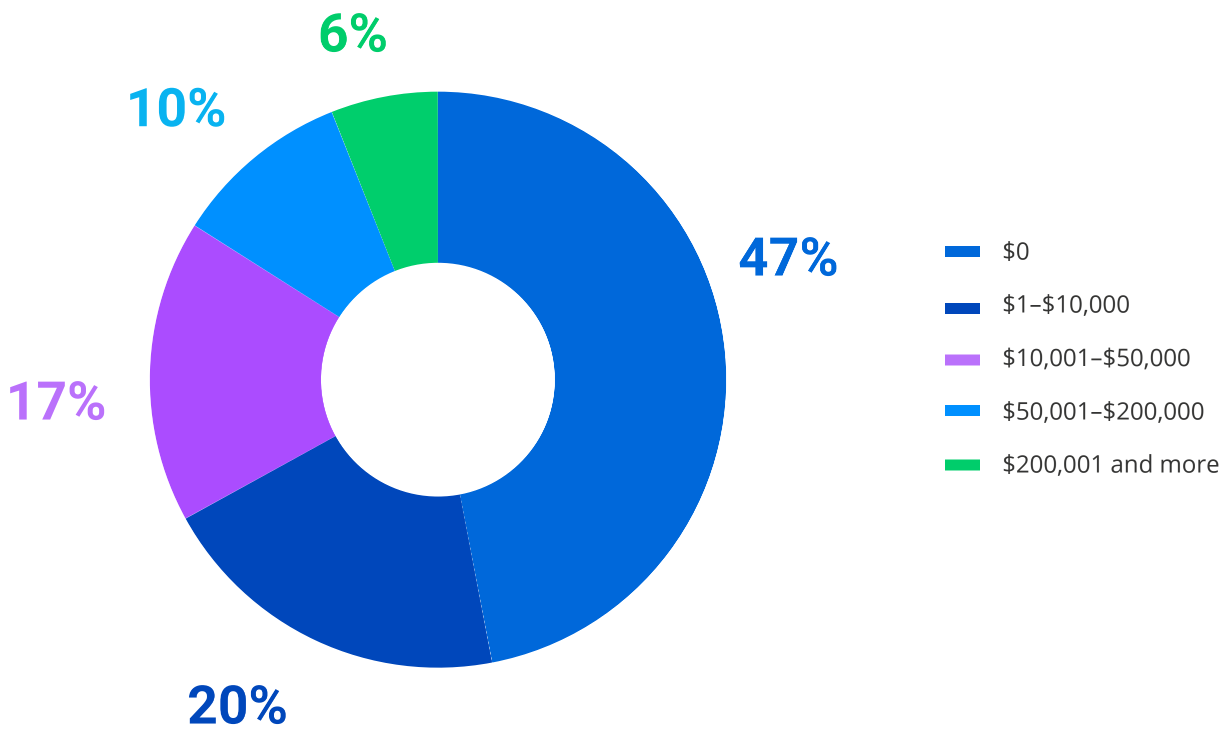


40% of organizations that suffered a data breach faced unplanned expenses as a result.

BREACH COSTS

Even though not every attack results in financial damage, some can be quite costly. Indeed, nearly 1 in 6 (16%) of organizations estimated their financial damage from cyberthreats to be at least $50,000.

Estimated financial damage due to cyberthreats

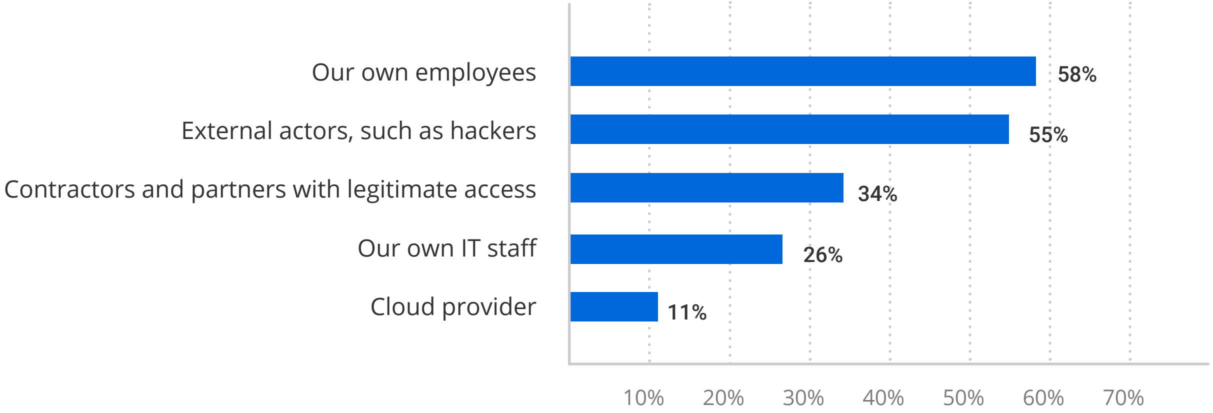


Nearly 1 in 6 organizations reported at least $50,000 in financial damage from cyberthreats.

THREAT ACTORS

To build an effective security architecture, it is crucial to assess who poses a threat. It turns out that IT pros are almost equally concerned about their own employees and external adversaries. Considering that 43% of respondents cited employee mistakes or negligence as the main challenge to data security, it is no surprise that the internal threat is top of mind.

Who poses the biggest risk to your data security?

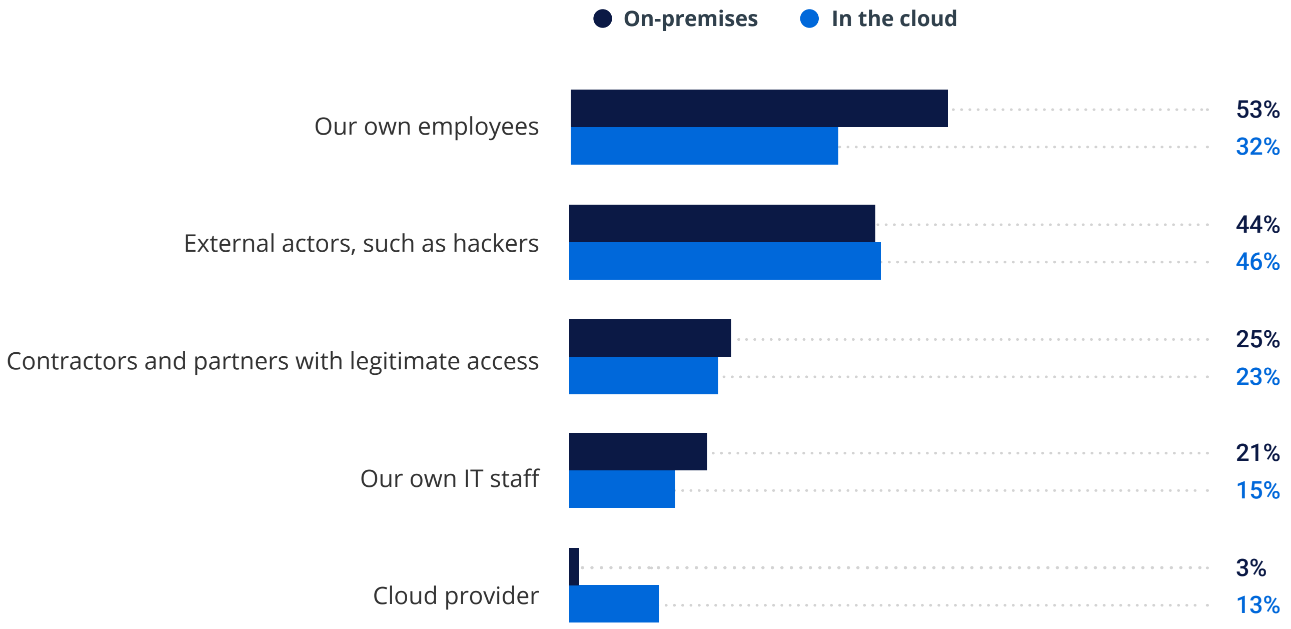


TIPS FROM DMITRY SOTNIKOV ON **HOW TO MAKE IT EASIER FOR END USERS TO STAY SAFE AND AVOID RISKY WORKAROUNDS:**

- Enforce the least-privilege principle with an identity governance and administration (IGA) tool that helps ensure accurate provisioning, re-provisioning and deprovisioning of users’ access.
- Make it easy for admins to request the privileged access they need to complete particular tasks and automatically remove that access immediately afterward.
- Build an automated workflow so business users can simply request the access they need and data owners can grant or deny those requests.
- Implement single-sign-on (SSO) to reduce the need to authenticate separately for every system or application.
- Implementing password policy and centrally-managed password vaulting software, particularly for those systems that cannot support an organization-wide SSO program, makes it easy for users to create strong, unique passwords and to access resources without the headache of memorizing (or worse, writing down) their various credentials.

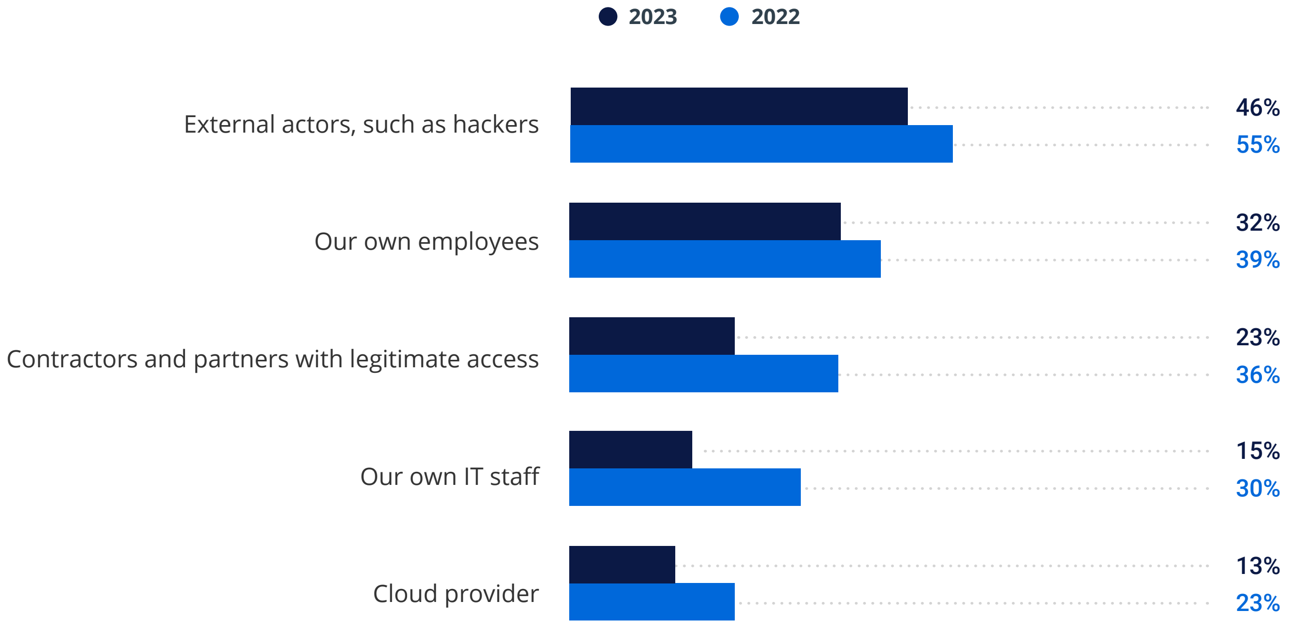
The survey also revealed that organizations are much more concerned about their own employees in regard to data security on premises than in the cloud; hackers topped the list for cloud infrastructure.

Who poses the biggest risk to your data security?



Concerns about threat actors in the cloud shifted significantly from the 2022 survey. In particular, while 30% of respondents chose their own IT staff as a top threat last year, only 15% picked that option this year.

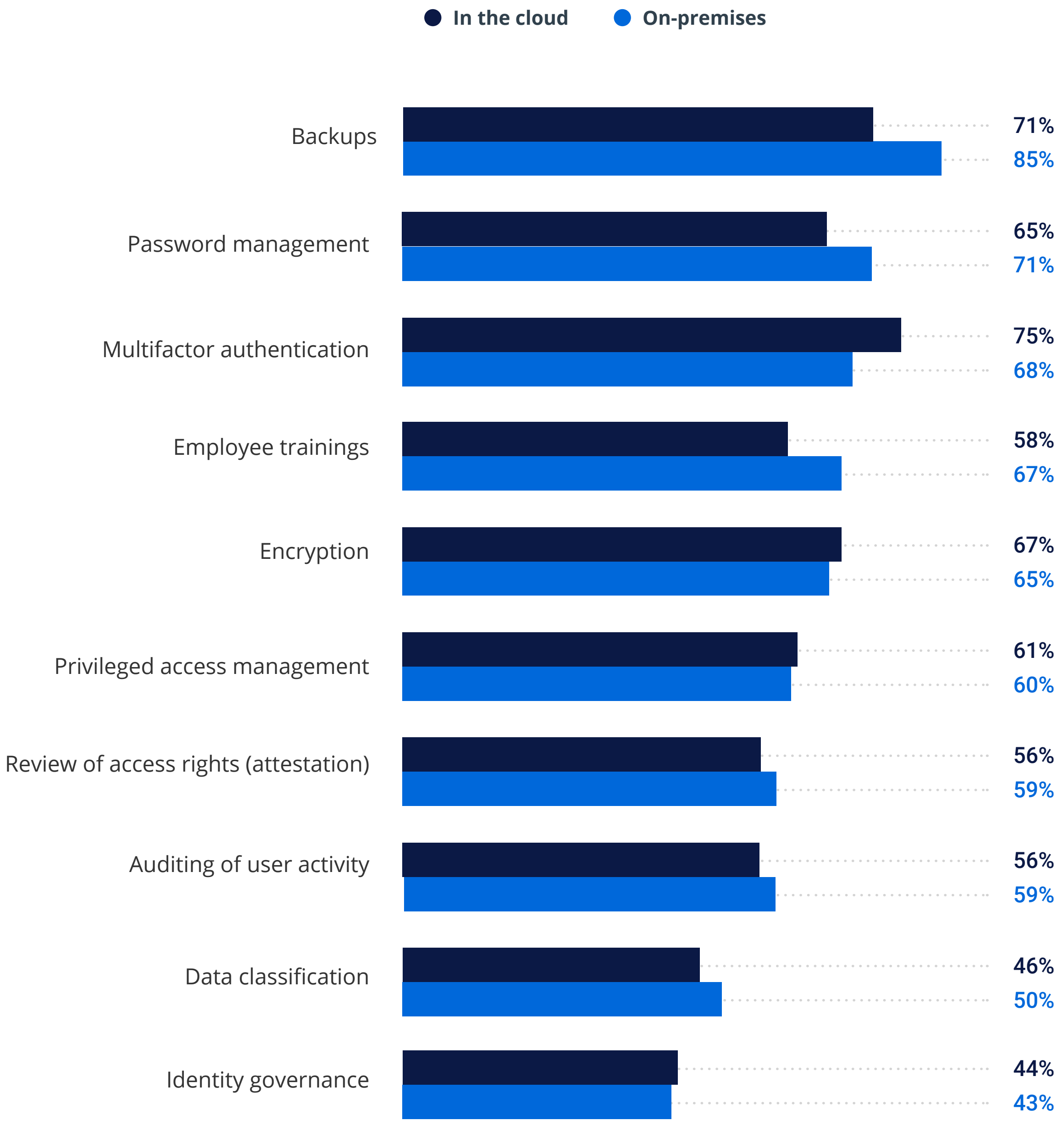
Who poses the biggest risk to your cloud data security?



CURRENT SECURITY MEASURES

We asked what measures our respondents take to protect their data in the cloud and on premises. We discovered that they do treat these parts of their IT environment differently. On premises, the three most common security measures being used are backups, password management and multifactor authentication (MFA); for the cloud, MFA topped the list, followed by backups and encryption.

What measures do you already take to protect your data?



BACKUPS

It is no surprise that backups topped the list of security measures: Security pros are always ready for a worst-case scenario. Dmitry Sotnikov offers the following backup best practices:

- **Limit access to backup systems** by implementing least privilege approach so no account compromise can lead to a compromise of a backup system.
- **Back up data regularly** to minimize how much of it will be lost it in the event of an attack.
- **Store backups offline** and away from a common network to make it more difficult for attackers to access backups. A cloud-based backup service is another option.
- **Encrypt backups** to complicate data extraction even if an attacker does gain access to the backups.
- **Test backups regularly** to identify any problems, solve those in a timely manner and make sure backups are working properly.
- **Use a disaster recovery plan** to recover from a data loss event quickly and effectively. The plan should include steps for restoring data, rebuilding systems, and getting business back on track.
- **Use audit and threat management tools** to reduce the scope of attacks and to evaluate which systems got compromised and need to be restored.
- **Use file integrity monitoring, change management, baselining tools** to identify which systems got compromised on the infrastructure level.

PASSWORD MANAGEMENT AND MFA

It is also no surprise that password management and multifactor authentication ranked high on the list of security measures.

> **Compromised passwords are one of the most common initial attack vectors. Adversaries frequently have success using lists of common passwords, as well as databases of leaked passwords because people often reuse the same credentials across sites. MFA gives significant protection against such attacks by adding another layer of defense; password management solutions make it easier for users to choose strong and unique passwords; and SSO reduces the number of passwords users need to manage and remember.**

Dmitry Sotnikov

VP of Product Management at Netwrix

EMPLOYEE TRAINING

Cybersecurity training is another common practice that can be quite effective. Users are any organization’s largest attack surface, so identity security should stay top of mind for every security team.

TIPS FROM DMITRY SOTNIKOV FOR EFFECTIVE SECURITY TRAINING:

- **Make it mandatory** for all employees regardless of their role in the organization.
- **Make it relevant** to the specific needs of the organization and the employees.
- **Make it engaging** and easy to understand.
- **Make it ongoing**, security training should not be a one-time event.
- **Measure the effectiveness** to ensure that it is having the desired impact.

However, he adds this caution:

> Do not rely on security training. Reduce your attack surface by strictly enforcing least privilege and replacing standing privileged accounts with ephemeral access. While training can reduce the chance of users making security mistakes, it does not eliminate that risk. Minimizing the privileges granted to each account reduces the damage that can result from account compromise.

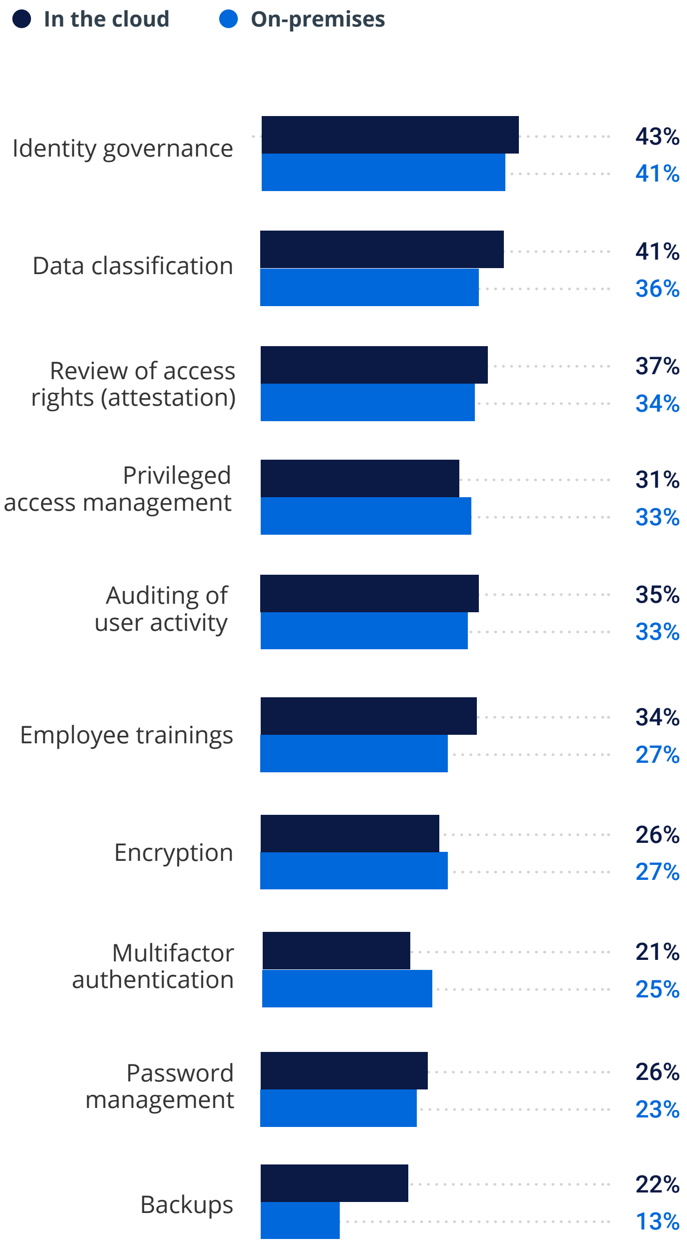
Dmitry Sotnikov
VP of Product Management
at Netwrix

PLANS FOR FUTURE SECURITY MEASURES

ORGANIZATIONAL PRIORITIES

Identity governance topped the list of measures that organizations plan to implement to improve cybersecurity both on premises and in the cloud.

What measures do you plan to implement to protect your data?



> **Three of the top four planned security measures are closely related: Identity governance, review of access rights (attestation) 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.**

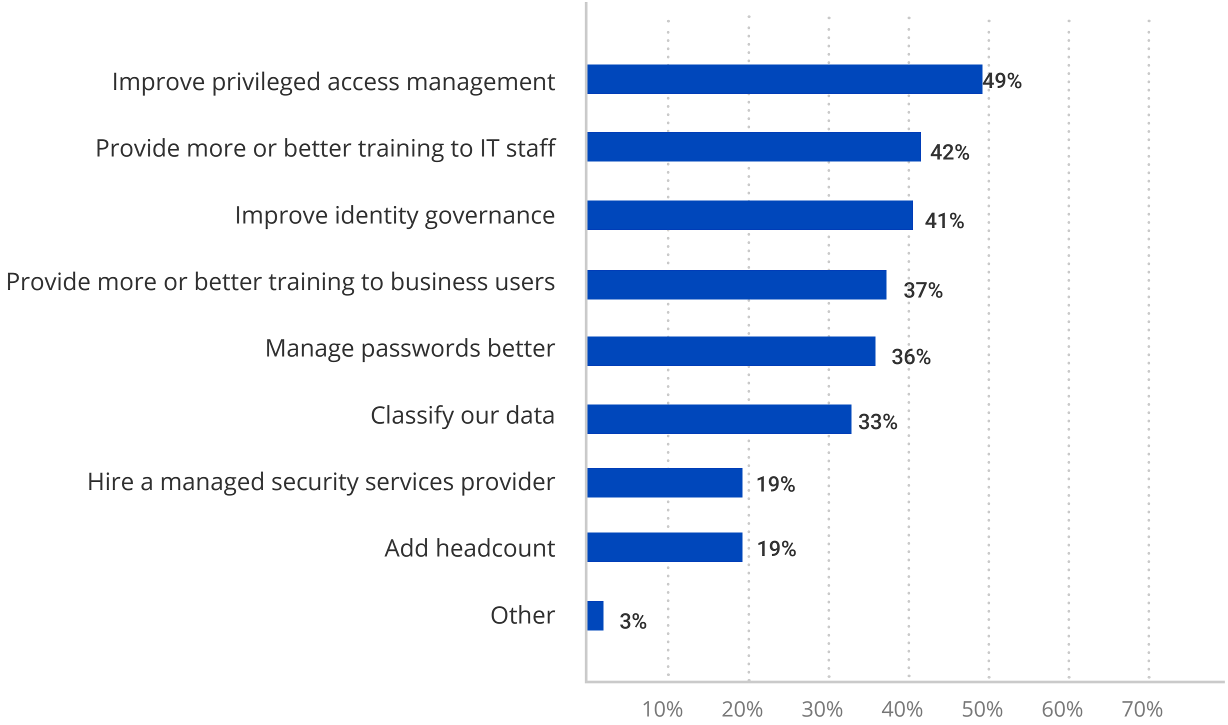
Dirk Schrader

VP of Security Research at Netwrix

IT PRO PRIORITIES

Priorities for future security measures would shift a bit if IT pros could decide on their own. PAM was their top choice, followed by better IT training and better identity governance.

If you had a chance to make a decision on your own, what measures you would take to enhance your organization's cybersecurity posture?



> **IT professionals understand that reducing the attack surface is fundamental to cybersecurity. In particular, ensuring that employees use administrative accounts responsibly can help organizations avoid costly errors and insider attacks. Even better, PAM solutions can replace standing administrative accounts with ephemeral accounts that have just enough rights for the task at hand — nearly eliminating the privileged account attack surface altogether.**

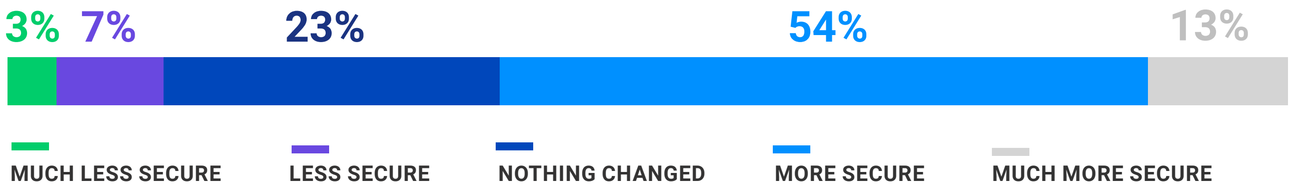
Dmitry Sotnikov

VP of Product Management at Netwrix

MOST TRUSTED SECURITY MEASURES

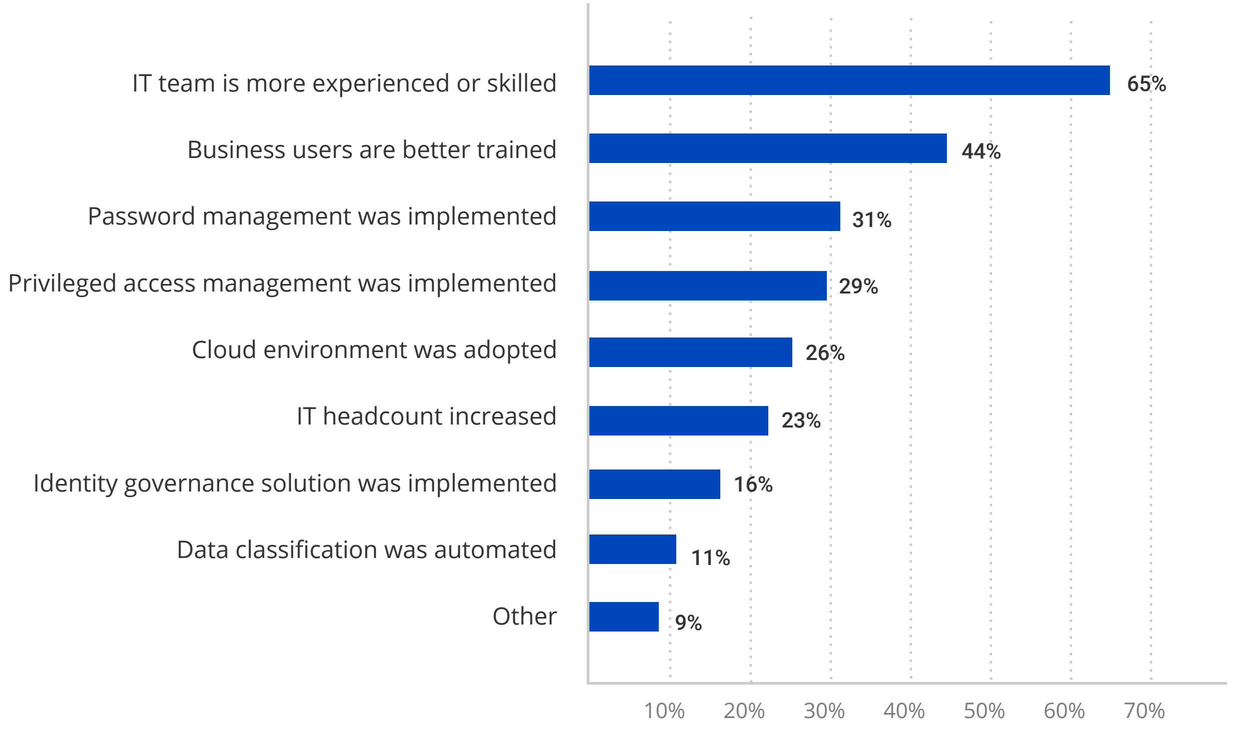
With all the hard work IT teams are doing to keep their organizations safe, we asked them to share how they really feel about the current state of cybersecurity. 67% of respondents say they are "more secure" or even "much more secure" now than they were a year ago.

How do you feel about your organization's security today vs. one year ago?



Then we asked them to clarify what exactly improved their cybersecurity posture. By a large margin, they said it was because both IT teams and business users are now better trained.

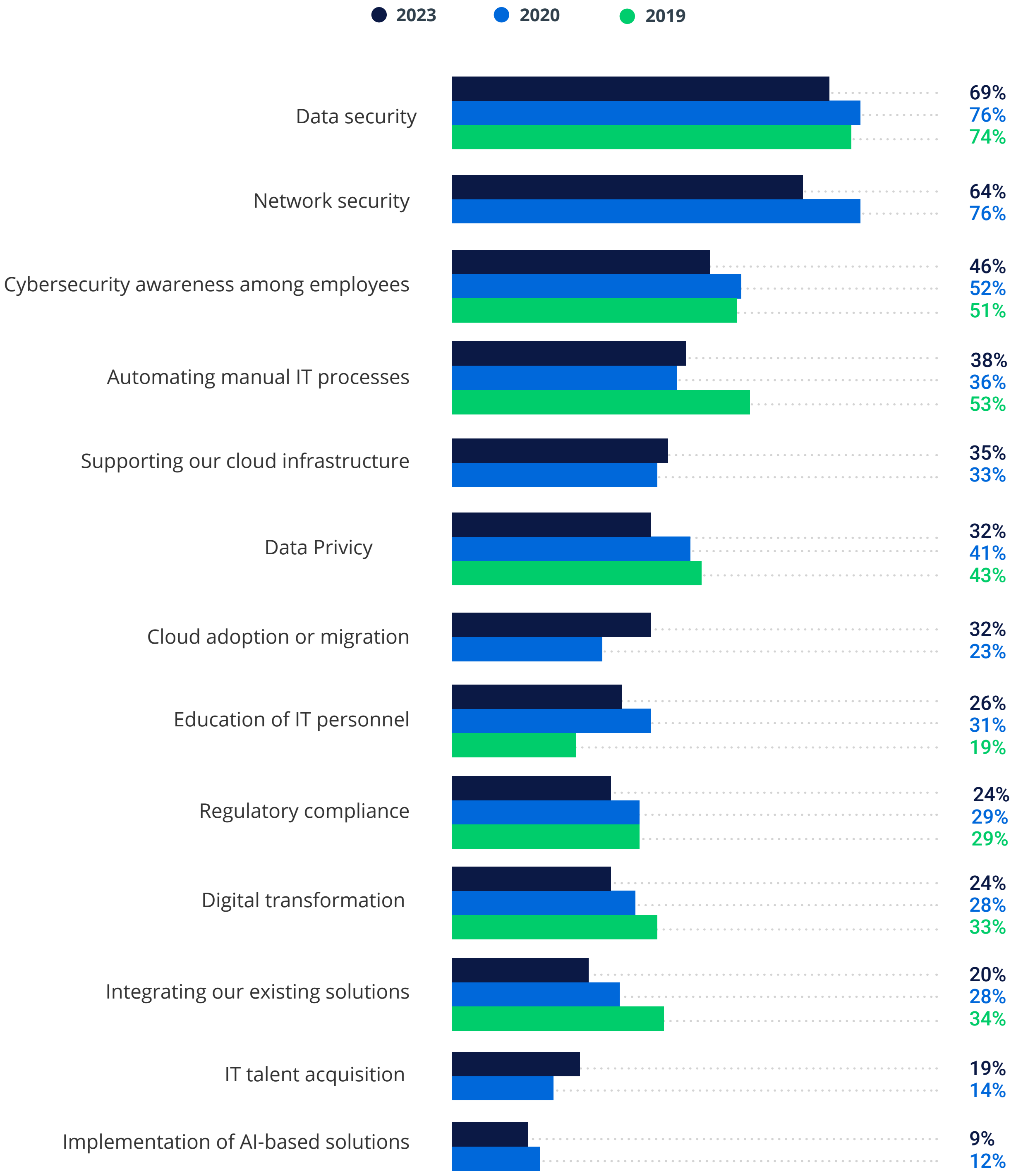
What happened to improve the security posture of your organization?



BROADER IT PRIORITIES

To assess the cybersecurity landscape at a high level, we asked respondents about their organization's top IT priorities for 2023. We compared the results with those from 2019 (before the Covid-19 pandemic) and 2020 (when lockdowns were in full swing). The main areas of concern stayed the same: data security, network security and cybersecurity training. Two areas that gained ground were cloud adoption and supporting the existing cloud infrastructure.

What are your organization's IT priorities for 2023?



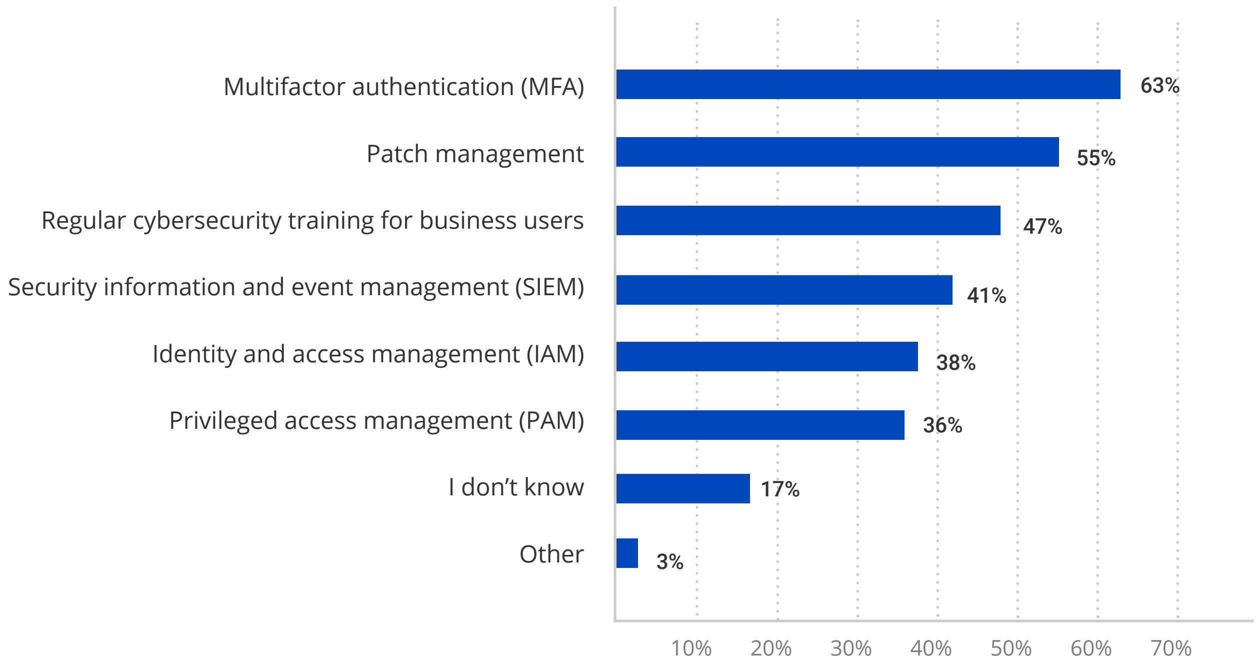
CYBER INSURANCE

Cyber insurance is meant to transfer the risk of financial loss resulting from a data breach to an insurance provider. No policy can restore an organization's data or operations, but an insurance payout can defray the financial impact or even prevent bankruptcy. It turns out that this approach to risk management is quite popular: 44% of organizations are insured and 15% plan to purchase a policy within the next 12 months.

59% **of organizations have a cyber insurance policy or plan to purchase one within 12 months.**

We asked the respondents with cyber insurance what requirements they had to meet in order to qualify for a policy. The most requested measure was multifactor authentication, followed by patch management and regular security training for business users.

What requirements did your organization have to meet in order for the insurance company to issue a policy?



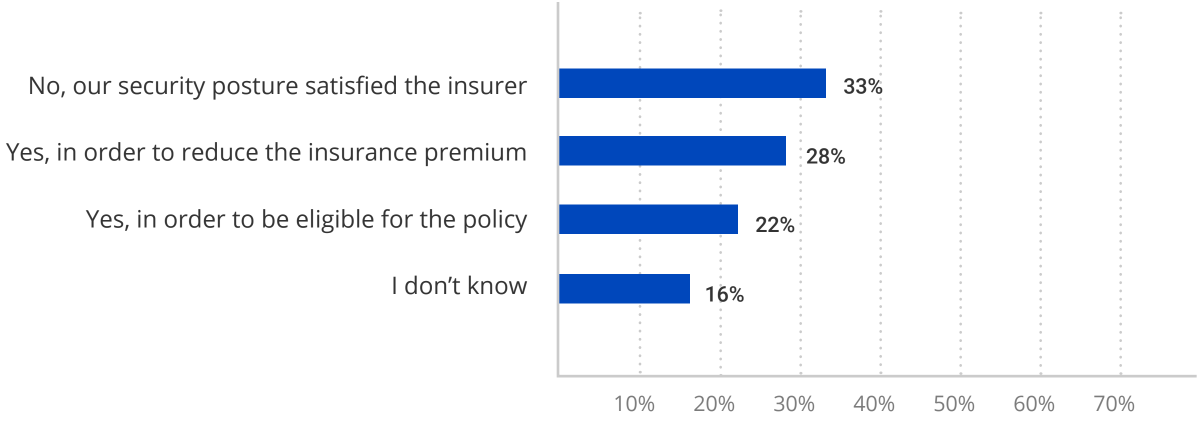
> **Both MFA and patch management have long been recognized as best practices that substantially improve an organization's security posture. Indeed, they help defend against two of the most common attack vectors: account takeover and exploitation of known vulnerabilities. So, it is not surprising that insurance companies check that organizations have implemented these core security measures**

Dirk Schrader

VP of Security Research at Netwrix

Nearly 3 in 10 (28%) organizations that have cyber insurance made changes in order to reduce their premium — and 22% had to improve their security posture to even be eligible for the policy.

Did you make any changes in order to meet the requirements of the insurance company?



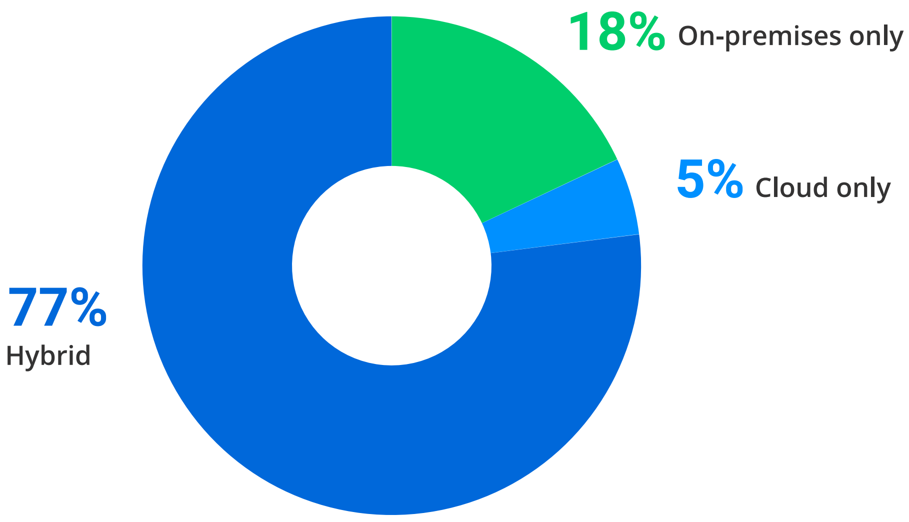
One in five (22%) of organizations had to improve their security posture to be eligible for their cybersecurity policy.

APPENDIX 1. 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 73% of respondents say they have a hybrid infrastructure, this number is higher for the enterprise sector (77%). What's more, the share of those organizations which have a hybrid environment is even larger for organizations with over 10,000 employees (88%).

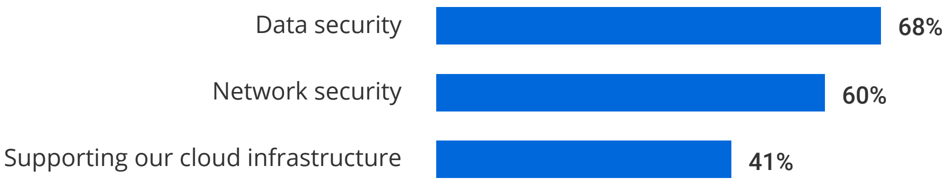
IT Architecture: enterprises



IT PRIORITIES

The two main IT priorities are the same for organizations of all sizes: data security and network security. Support of a cloud infrastructure ranked third for the enterprise sector while for respondents overall, cloud associated goals landed in the middle of the list.

Top IT priorities for the enterprise sector

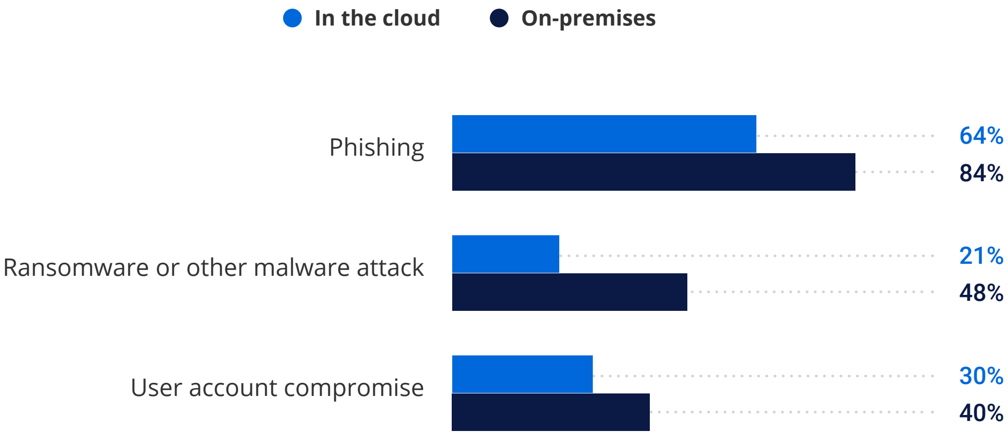


SECURITY INCIDENTS

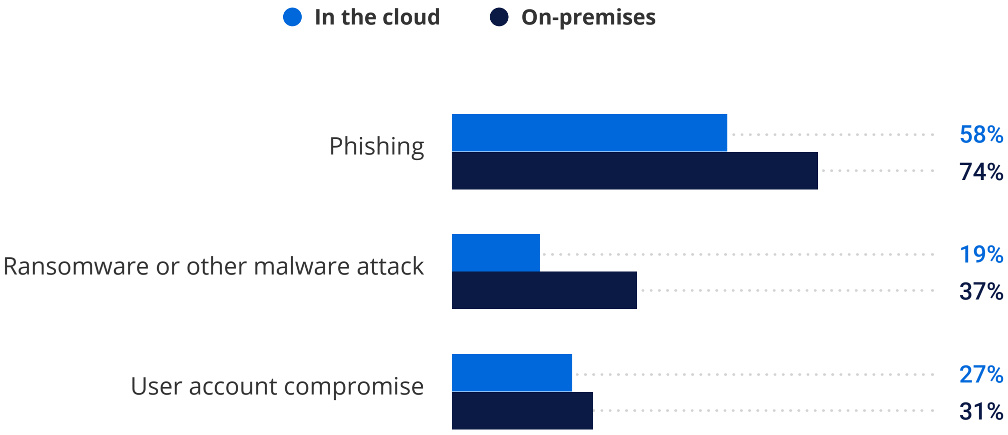
65% of organizations in the enterprise sector suffered a cyberattack within the last 12 months, which is similar to the results among companies of all sizes (68%). The most common security incidents are the same: phishing, ransomware, and user account compromise.

However, the largest organizations are targeted more often with ransomware or other malware attacks: 48% of enterprises experienced this type of security incident on premises compared to 37% among organizations of all sizes.

Most common security incidents in the enterprise sector



Most common security incidents in organizations of all sizes



Smaller companies often underestimate their risk of attack, reasoning that cybercriminals tend to target enterprises because they store more intellectual property (IP) and other sensitive data. To the contrary, our survey reveals that the risk of cyberattack is virtually the same regardless of company size — every organization has valuable data, such as customer and employee information, and is therefore a target for attackers.

Dirk Schrader

VP of Security Research at Netwrix

However, the enterprise sector suffers malware attacks at a higher rate than smaller organizations. After all, ransomware operators want to maximize their profits, so they consider which organizations are most likely to pay a ransom to reduce business downtime — and the larger an organization is, the costlier an operational disruption will be.

Dmitry Sotnikov

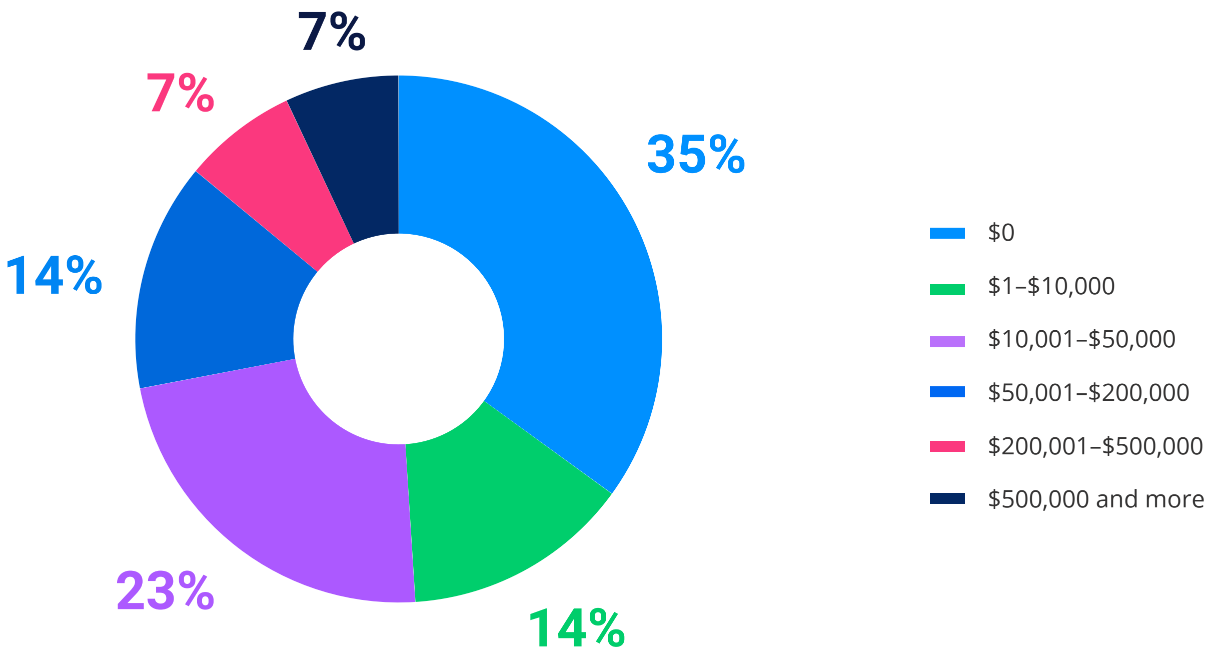
VP of Product Management at Netwrix

COST OF CYBERATTACKS

The enterprise sector also reports larger expenses as a result of cyberattacks than their smaller counterparts. Indeed, 28% of enterprises estimated their financial damage from cyberthreats to be at least $50,000, compared to just 16% among organizations overall.

To address the risk of financial loss due to cyberthreats, 58% of enterprises already have a cyber insurance policy or plan to purchase one within the next 12 months.

Estimated financial damage due to cyberthreats in the enterprise sector



38% of enterprises opt to enhance their security posture in order to reduce their insurance premium, compared to 28% among organizations of all sizes.

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 makes data security easy. Since 2006, Netwrix solutions have been simplifying the lives of security professionals by enabling them to identify and protect sensitive data to reduce the risk of a breach, and to detect, respond to and recover from attacks, limiting their impact. More than 13,000 organizations worldwide rely on Netwrix solutions to strengthen their security and compliance posture across all three primary attack vectors: data, identity, and infrastructure.

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