netwrix

2022

Cloud Data Security Report

EXECUTIVE SUMMARY

Cloud infrastructure has become an integral part of daily workloads for millions of organizations worldwide. After the sudden shift to remote work in 2020, cloud adoption is still in progress and, as this report proves, is expected to continue over the next 12-18 months. Netwrix Research Lab has updated the Cloud Data Security Reports from 2020 and 2019 to reflect the evolution of cloud security. In March 2022 we surveyed 720 IT professionals all over the globe via an online questionnaire. This report will help organizations concentrate their security efforts on what really matters and highlight the main obstacles on their way to safe cloud computing.

CLOUD ADOPTION

Organizations turned to the cloud mainly to reduce costs and to improve security. 80% of those who use the cloud store sensitive data there. The biggest challenge for cloud adoption, named by 41% of respondents, is integration with their existing IT environment.

INCIDENT DETECTION

84% of respondents believe the time required to detect the incident either didn't change or dropped. This is how they assessed their progress within the last year. A deeper dive reveals that the average detection time for most types of attacks has actually increased since 2020. The most significant slowdowns can be seen for discovery of supply chain compromise and ransomware attacks.

SECURITY INCIDENTS IN THE CLOUD

53% of survey respondents suffered a cyberattack within the last 12 months. Phishing was the most commonly experienced incident – 73% of respondents confirmed that they had been victimized by this type of attack within the last year. Moreover, targeted attacks on cloud infrastructure increased significantly: 29% of respondents suffered this type of attack in 2022, compared to 16% in 2020.

DATA BREACH CONSEQUENCES

Data breaches are getting costlier. This year, 49% of respondents said that an attack led to unplanned expenses to fix security gaps, up from 28% in 2020. The share who faced compliance fines more than doubled (from 11% to 25%), as did the number who watched as their company valuation dropped (from 7% to 17%).

CLOUD SECURITY MEASURES

More than half (55%) of respondents said that external actors are the main threat for their IT environment. Multifactor authentication (MFA) and cloud backup topped the list of protection measures. Both saw increases since 2020: MFA adoption grew from 57% to 69% and backups increased, albeit marginally, from 58% to 63%.

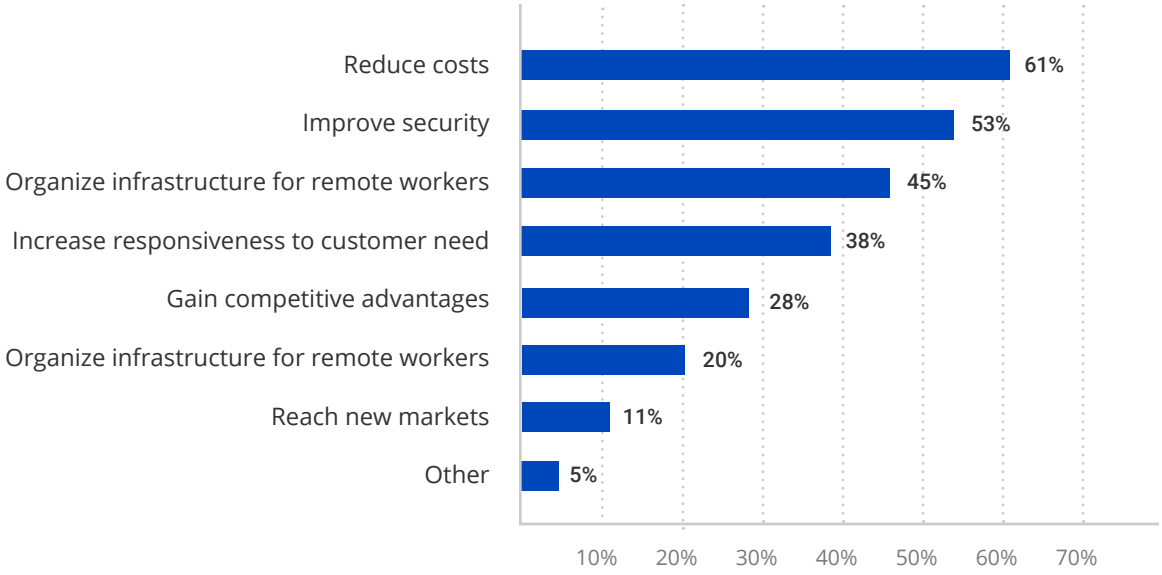
BUDGETING

49% of our respondents stated that their budget for cloud security increased in 2022. Moreover, organizations are devoting more of their larger cybersecurity budgets to cloud security: On average, 32% of the cybersecurity budget is now spent on cloud security, compared to 27% in 2020. This means a 23% increase of money being spent on cloud security in 2022 than in 2020.

CLOUD ADOPTION GOALS AND CHALLENGES

The survey found that the top two goals of cloud adoption are to reduce costs and improve security. Supporting remote workers ranked third, which indicates that the pandemic may have accelerated cloud adoption, but cost-efficiency and security are the most significant drivers.

Primary cloud adoption goals



WHAT'S IN THE CLOUD?

On average, organizations report that 41% of their workloads are already in the cloud, and they expect that share to increase to 54% by the end of 2023.

What percentage of your workloads are in the cloud today?

41%

What percentage of your workloads are planned to be in the cloud in 12-18 months?

54%

Storage of sensitive data in the cloud hasn't changed much since the pandemic hit in 2020; however, the numbers for the two top categories are still lower than they were in 2019. For example, the percentage of organizations storing customer data in the cloud dropped from 50% in 2019 to 44% in 2020 and then remained level in 2022; employee data dropped from 50% in 2019 to 42% in 2020, and then inched up to 44% in 2022. On the other hand, the share of those who store corporate financial information in the cloud rose from 26% in 2019 and 2020 to 35% in 2022.

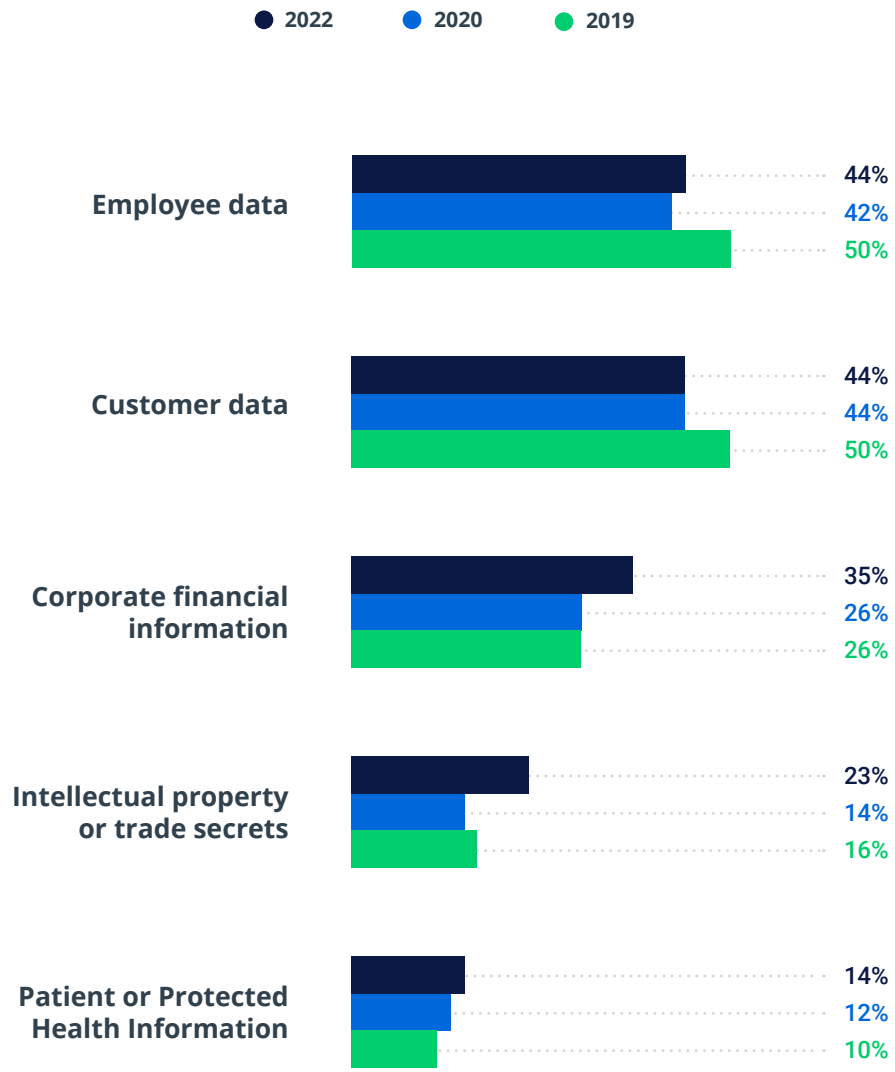
In 2019, cloud adoption seemed like a magic wand that would reduce costs, increase flexibility, and accelerate business processes. But with the abrupt shift to remote work in 2020, IT teams reassessed the risks and pulled some customer and employee PII back on premises, a trend that plateaued in 2022. However, more organizations now store other types of sensitive data, such as corporate financial data and IP, in the cloud than before, which shows that IT teams believe that they have improved their cloud skills and learned how to use it effectively and securely.

Dirk Schrader

VP of Security Research at Netwrix

80% of respondents store sensitive data in the cloud. The most common types are the PII of employees and the PII of customers.

Types of sensitive data organizations store in the cloud



ONLY 20% of organizations which use the cloud don't store any sensitive data there

WHAT ARE THE BIGGEST CLOUD CHALLENGES?

The biggest challenge for rapid cloud adoption, named by 41% of respondents, is integration with their existing IT environment. The second factor impeding the process is lack of IT staff.

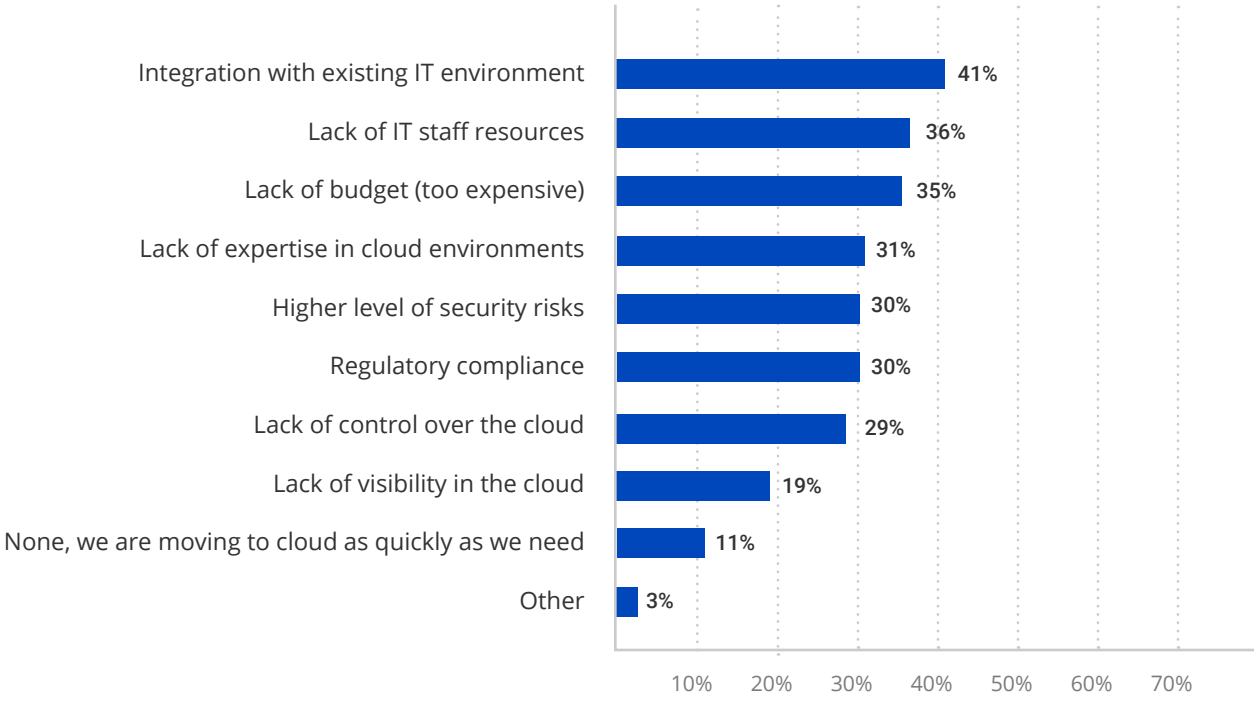
Reducing costs is the primary reason to move to the cloud for 61% of respondents, but 35% said that the expense of cloud adoption has slowed their move to the cloud. "This is a tricky thing about cloud infrastructure: Cloud and on-premises infrastructures are too different to try and just move every workload as is; indeed, a lift-and-shift approach can lead to significant extra expenses and even require costly architecture redesign if issues are found late in the process," comments Mike Paye, VP of Research and Development at Netwrix. "For example, if you have an application that relies on a SQL backend, it is possible to reproduce it exactly in the cloud with a virtual machine running Microsoft SQL Server. However, this will likely be both the least efficient and the most expensive architecture you can think of. From this perspective, it seems that some of the respondents who say their cloud migration was too expensive might lack sufficient expertise with cloud environments."

Still, the expense of a cloud infrastructure can be harder to predict than those in an on-premises environment.

When you need a server, the cost calculation is rather easy: Add together the price of the server itself, the electricity, the IT team salary. When it comes to the cloud, you receive a bill for the amount of resources used for actual workload. Without controls in place, consumption and the bill will increase every month. That is why it's crucial to keep an eye on what the organization currently needs and maintain a flexible architecture so you can turn off and on the relevant cloud options.

Mike Paye
VP of Research and Development
at Netwrix

Factors that slow down cloud adoption

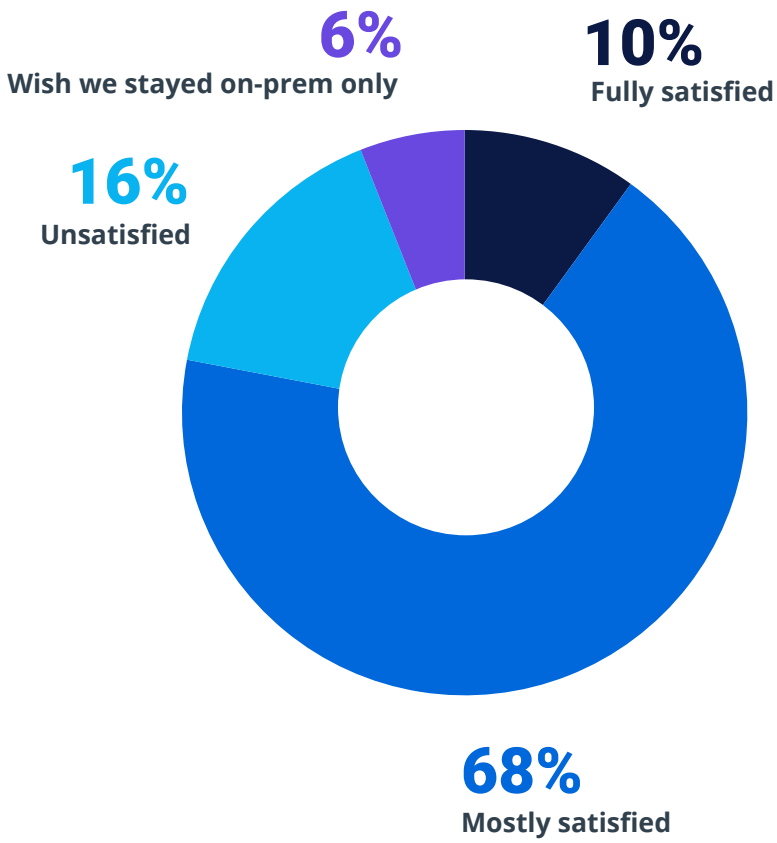


The biggest issues for CIOs are lack of expertise in cloud and integration with existing IT environment – these reasons topped the list for 33% of CIOs asked.

SECURITY INCIDENTS IN THE CLOUD

More than half (53%) of respondents picked security improvement as their main goal for the cloud adoption. And it looks like they achieved that objective: 78% of respondents say they are satisfied with their organization's cloud security.

Satisfaction with cloud security



25% of CISOs are unsatisfied with their organization's cloud security

ATTACKS IN THE CLOUD

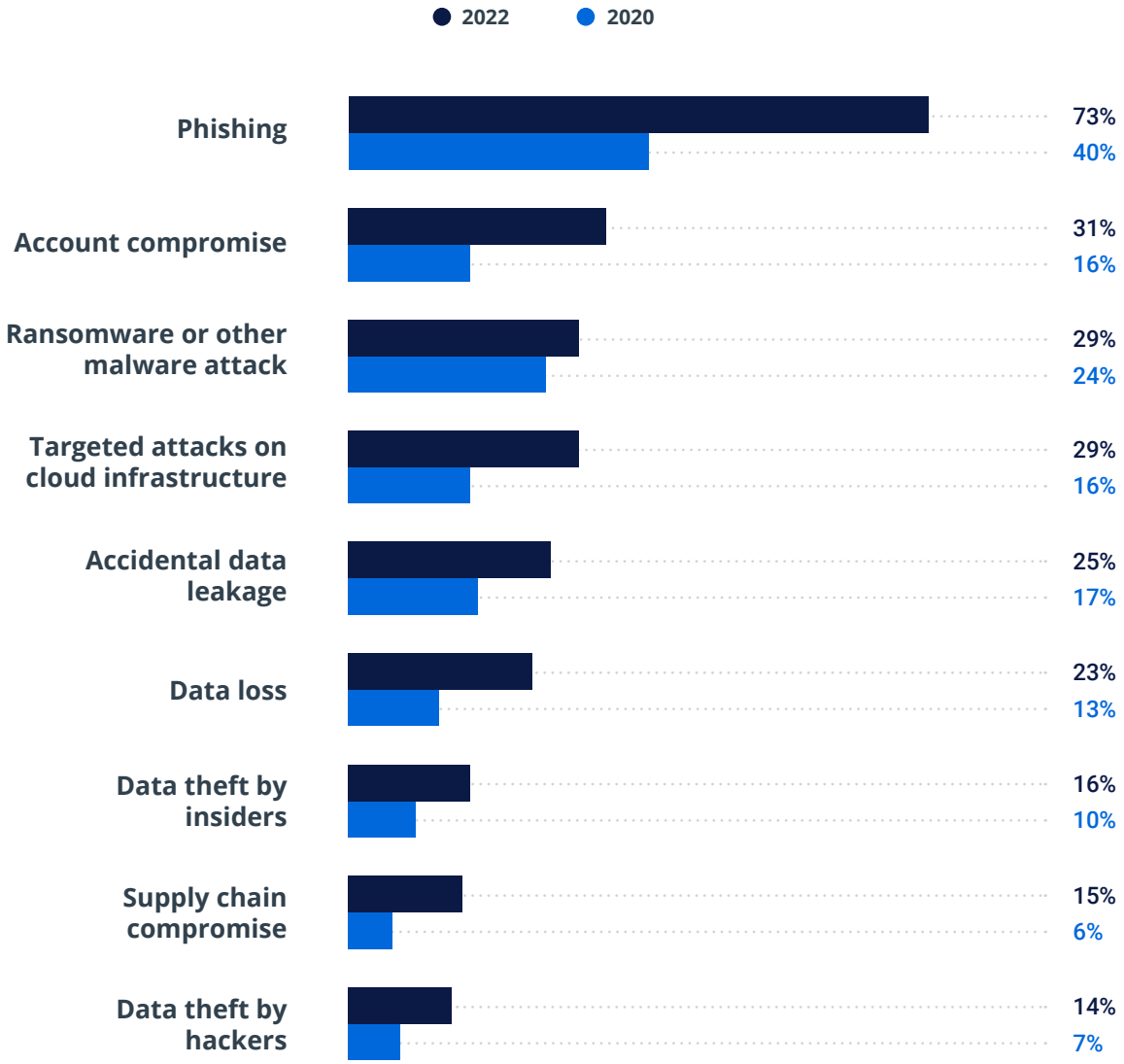
CIO from Canada:

"Attacks are not a matter of if, but when."

53% of survey respondents suffered a cyberattack within the last 12 months. Security professionals know that it's impossible to achieve full cybersecurity, which means that the remaining 47% 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 and compared these answers with the results from 2020.

Most common cloud security incidents



Phishing was the most commonly experienced incident. Although it was also the leader in 2020, the percentage of organizations that suffered this type of attack nearly doubled, from 40% to 73%. Moreover, 63% of respondents said they experienced this type of an attack multiple times.

Targeted attacks on cloud infrastructure also increased significantly: 29% of respondents suffered this type of attack in 2022, compared to 16% in 2020. This stands to reason since the more workloads that are moved to the cloud, the more targeted attacks on cloud environments we will see.

In 2022, 31% of respondents said they experienced a compromised account, up from only 16% in 2020. This could be the result of negligence by remote workers (e.g., logging in through public Wi-Fi) and a wider attack surface due to necessity of granting remote access to many people. Moreover, people often use the same — and not always strong — password for several resources and resist multifactor authentication because they find it annoying.

Mike Paye
VP of Research and Development
at Netwrix

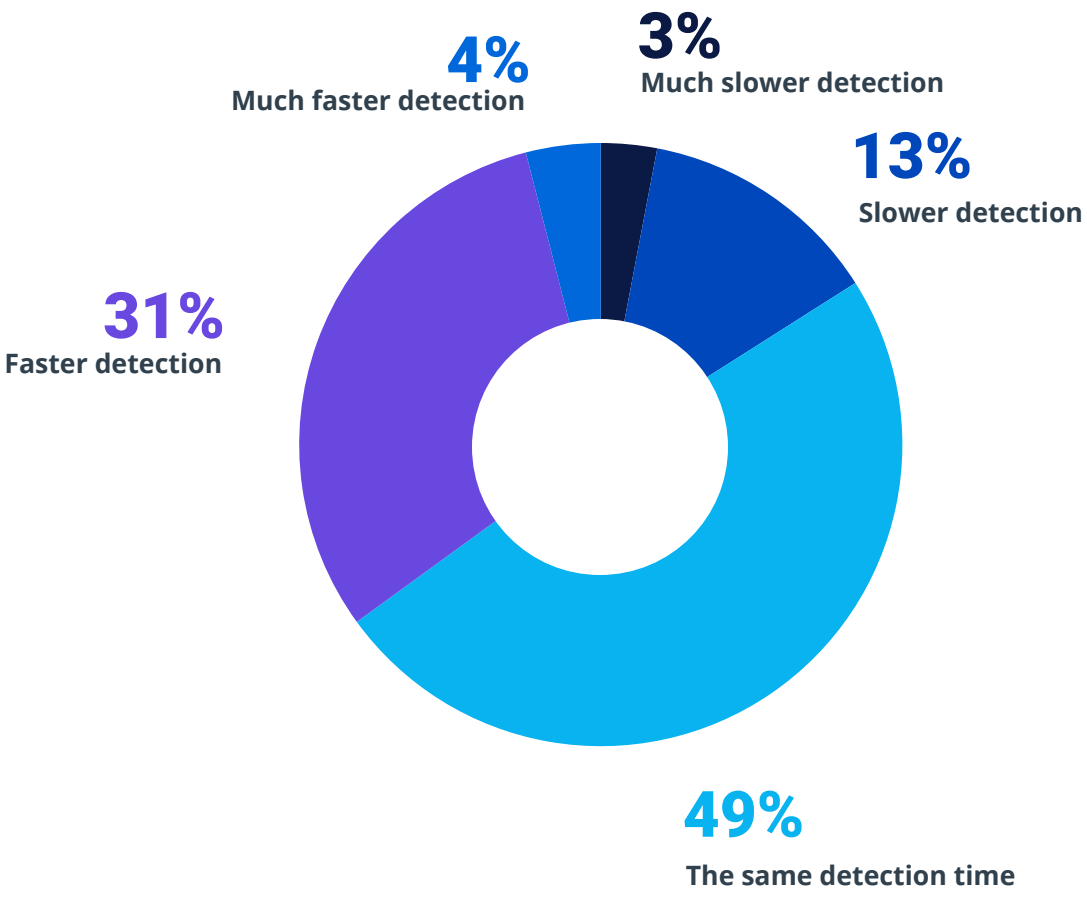
In 2022, the third most common type of attack was ransomware or other malware. The share of respondents who experienced such incidents increased slightly since 2020, from 24% to 29%, and is in Top-3. The number of attacks increased globally in part because cryptocurrency gave threat actors a far less traceable way of receiving ransom money. Moreover, ransomware-as-a-service now makes it easy to scale this 'business'.

Dirk Schrader
VP of Security Research
at Netwrix

DETECTION TIME

Next, we asked whether the time required to detect an incident in the cloud changed compared to 12 months ago. More than a third of the respondents (35%) said that detection is now faster, while 49% said detection time hasn't changed.

Change in incident detection time



To dive deeper, we asked respondents how much time it took to discover and respond to the cloud security incidents they suffered in the past 12 months. The chart below compares those results with the data from 2020 to show which types of attacks have become easier to discover.

RANSOMWARE OR OTHER MALWARE ATTACK

DETECTION TIME	2020	2022
MINUTES	35%	35%
HOURS	51%	39%
DAYS	9%	19%
WEEKS	5%	3%
MONTHS AND MORE	0%	5%

PHISHING

DETECTION TIME	2020	2022
MINUTES	44%	42%
HOURS	42%	40%
DAYS	13%	12%
WEEKS	1%	3%
MONTHS AND MORE	0%	3%

TARGETED ATTACKS ON CLOUD INFRASTRUCTURE

DETECTION TIME	2020	2022
MINUTES	32%	31%
HOURS	51%	42%
DAYS	15%	17%
WEEKS	2%	4%
MONTHS AND MORE	0%	6%

DATA LOSS

DETECTION TIME	2020	2022
MINUTES	23%	25%
HOURS	42%	36%
DAYS	29%	24%
WEEKS	6%	9%
MONTHS AND MORE	0%	6%

ACCIDENTAL DATA LEAKAGE

DETECTION TIME	2020	2022
MINUTES	16%	22%
HOURS	23%	31%
DAYS	47%	28%
WEEKS	14%	12%
MONTHS AND MORE	0%	7%

DATA THEFT BY INSIDERS

DETECTION TIME	2020	2022
MINUTES	23%	20%
HOURS	27%	26%
DAYS	27%	28%
WEEKS	19%	14%
MONTHS AND MORE	4%	12%

DATA THEFT BY HACKERS

DETECTION TIME	2020	2022
MINUTES	16%	23%
HOURS	53%	30%
DAYS	21%	26%
WEEKS	0%	12%
MONTHS AND MORE	10%	9%

SUPPLY CHAIN COMPROMISE

DETECTION TIME	2020	2022
MINUTES	23%	20%
HOURS	53%	27%
DAYS	18%	30%
WEEKS	0%	12%
MONTHS AND MORE	6%	10%

ACCOUNT COMPROMISE

DETECTION TIME	2020	2022
MINUTES	20%	30%
HOURS	49%	36%
DAYS	24%	23%
WEEKS	7%	6%
MONTHS AND MORE	0%	5%

In response to the previous question, 84% of respondents said the time required to detect the incident either didn't change or was reduced — but this deeper dive reveals that the average detection time for most types of the attacks has actually increased since 2020. The most significant slowdowns can be seen for discovery of supply chain compromise and ransomware attacks.

Moreover, in 2020, only three types of attacks took months or more to be discovered; in 2022, every type of attack has a share of respondents who needed months or more to detect.

We do see progress for several attack types. 53% of respondents needed minutes or hours to detect accidental data leakage, versus just 39% in 2020. And the number of respondents who discovered account compromise in minutes increased from 20% in 2020 to 30% in 2022.

These results mean that attacks have become more sophisticated and harder to spot. Despite all the new tools that provide more visibility to security teams, it is still a challenge to detect signs of a threat actor in the IT environment. Point solutions leave security gaps as they operate separately. One way to solve this problem is to reduce the number of vendors and build the security architecture with a select group of trusted vendors, whose extensive portfolio of products do complement each other, and that are committed to collaboration across portfolio boundaries.

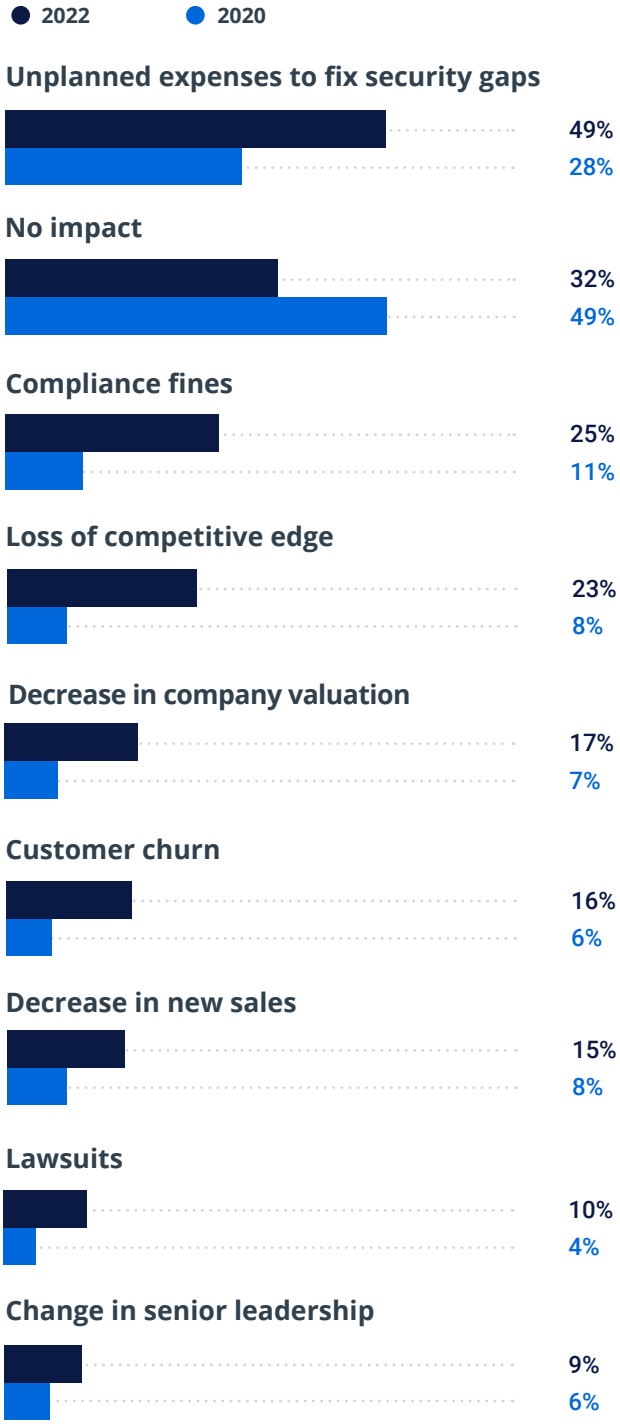
Dirk Schrader

VP of Security Research at Netwrix

DATA BREACH CONSEQUENCES

Not every attack is catastrophic. The truth is that in 32% of cases, the attack has no impact on business. However, that is a significant drop from 49% in 2020.

Data breach consequences

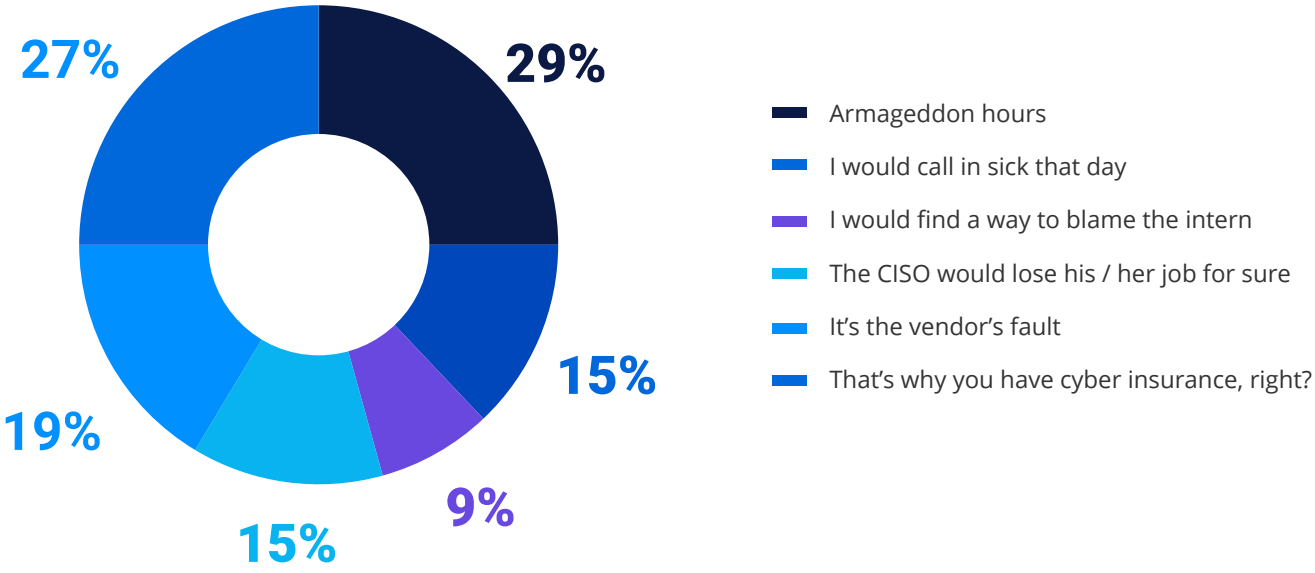


Data breaches are getting costlier. This year, 49% of respondents said that an attack led to unplanned expenses to fix security gaps, up from 28% in 2020. Similarly, those who faced compliance fines more than doubled (from 11% to 25%), as did the number who saw their company valuation drop (from 7% to 17%). Organizations shifting their value-generating processes to the cloud should be conscious of such statistics. These results should help CIOs and CISOs prove the necessity of additional budget to keep their organization safe. A resilient cybersecurity costs less than consequences of data breaches.

Dirk Schrader

VP of Security Research at Netwrix

Our respondents take their responsibilities very serious, so we added in a bit of levity to this year's survey just to ease the pressure for a moment. We asked how devastating would the breach be if happened in their cloud data storage.

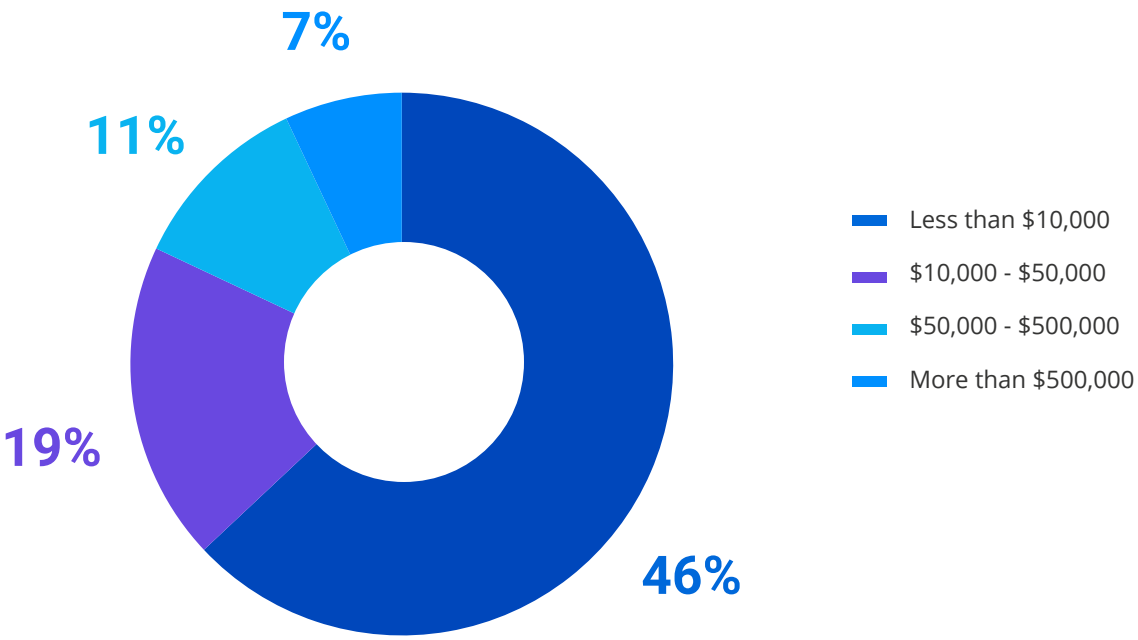


IT pros are no strangers to a good laugh. One respondent commented: "Data breach consequences? Some services do not work, so I will go to the beach." We admire the ability of security professionals to keep their calm (and a sense of humor) under any circumstances.

HOW MUCH DID THE BREACH COST?

Considering that 32% didn't see any impact on their business from the incidents they suffered, it is no surprise that most respondents (63%) estimated the harm from a data breach at less than $10,000.

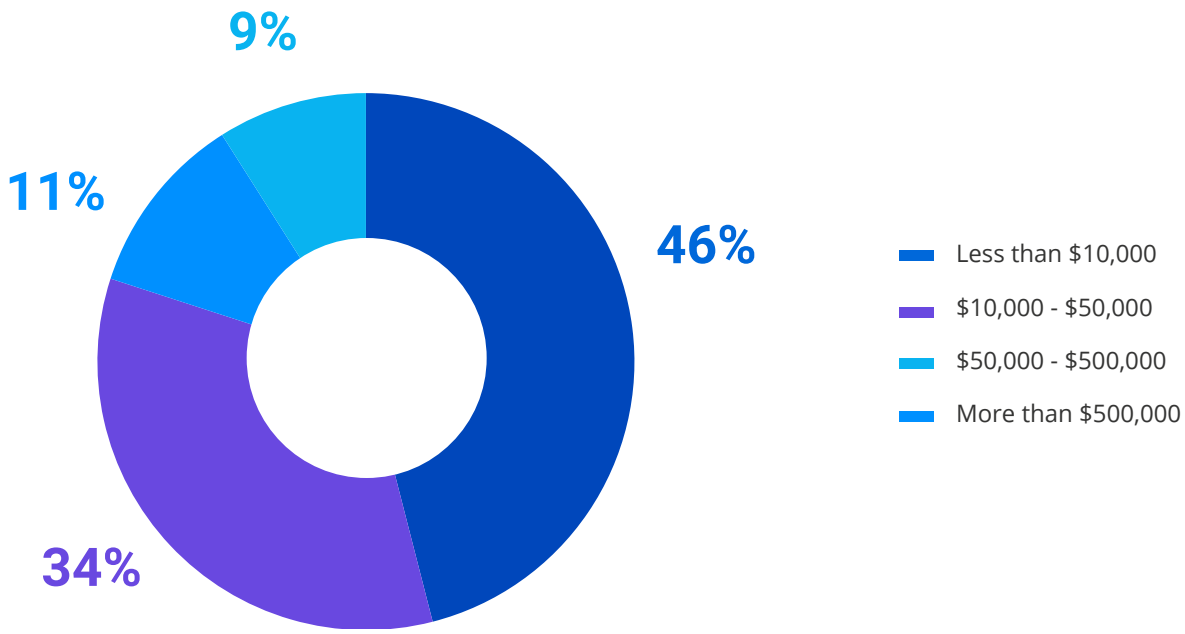
Estimated financial damage due to cyber threats



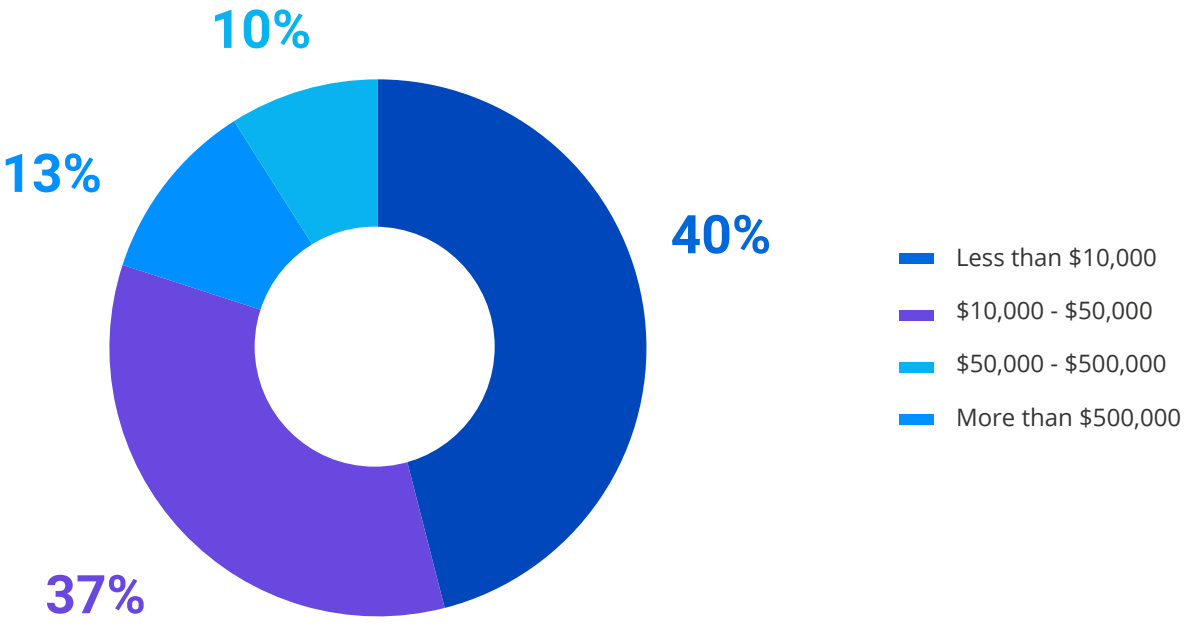
However, in large organizations (over 1,000 employees), data breaches are more likely to have expensive consequences. While most of those respondents in this group (46%) still estimate the damage at less than $10,000, 34% said it cost them $50,000–$500,000. Among the overall pool of respondents, only 19% estimated the damage to be that high.

Similarly, the share estimating the damage at more than $500,000 is the biggest in very large enterprises (over 10,000 employees) — 13% versus 7% overall. In short, the bigger an organization is, the more likely that the consequences of data breach will be expensive.

Large (1,000+ employees)



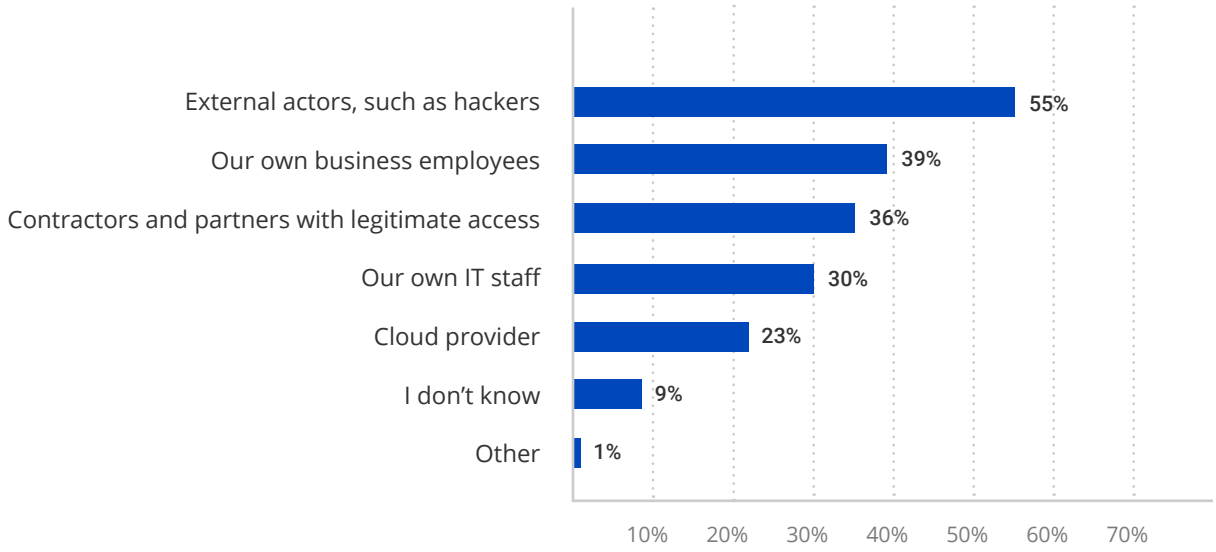
Very large (10,000+ employees)



CLOUD SECURITY MEASURES

Before diving into the security measures organizations implement to keep their data safe, we asked about whom they are most concerned. More than half (55%) of respondents said that external actors are the main threat for their IT environment, followed by their own employees (39%) who might be creating security gaps inadvertently as well as contractors and partners requiring legitimate access (36%).

Who poses the biggest risk to data security in the cloud?



Then we asked what measures our respondents take to protect their data in the cloud and compared their answers with the data from our previous report.

In 2020, the most common cloud security controls organizations reported were encryption (62%), auditing of user activity (58%) and employee training (58%). In 2022, the share of respondents using those measures is exactly the same.

In the current survey, multifactor authentication and cloud backup topped the list of protection measures. Both saw increases since 2020: MFA adoption grew from 57% to 69% and backups increased from 58% to 63%.

What measures do you take to protect your data in the cloud?

	NOT GOING TO DO	PLAN TO DO	ALREADY DO
Multifactor authentication	7%	24%	69%
Cloud backup	7%	30%	63%
Encryption	9%	29%	62%
Employee trainings	7%	34%	59%
Auditing of user activity	7%	35%	58%
Review of access rights (attestation)	8%	37%	55%
Data classification	17%	46%	37%
Remove sensitive files from the cloud	29%	37%	34%
Cloud access security broker	30%	46%	24%

99%

of CIOs either already conduct employee security training or plan to do so.

70%

of CISOs are auditing user activity in the cloud and 28% plan to start doing so.

ONLY

5%

of CISOs don't classify data in the cloud and don't plan to do so.

The least common security measure remains use of a cloud access security broker. Although CASBs are still not very popular, the share who plan to implement this option increased from 33% in 2020 to 46% now. Meanwhile, the number who said they would not use this approach dropped from 40% to 30%. One reason for the lack of interest in this control is that it has the vaguest ROI of all the choices on the list.

Dirk Schrader
VP of Security Research at Netwrix

Use of MFA is increasing because compromising user passwords remains a simple and effective attack tactic. Adversaries often have success using lists of the most common passwords, and they can also leverage databases of leaked passwords from other websites because people often reuse the same password across sites. Plus, with more employees working remotely, bad actors can more easily log into corporate systems without raising suspicion. MFA is the cheapest and most effective way to reduce the risk of account compromise. The increased implementation of regular cloud backups can be linked to the rising number of ransomware attacks. It should be kept in mind though that while data may be easily restored from backups, bad actors can still blackmail organisations and individuals alike by threatening to publish the data.

Mike Paye
VP of Research and Development at Netwrix

MEASURES TO PROTECT DATA IN THE CLOUD BY ORGANIZATION SIZE

Large (1,000+ employees)

	NOT GOING TO DO	PLAN TO DO	ALREADY DO
Multifactor authentication	5%	20%	75%
Employee trainings	4%	28%	68%
Encryption	7%	26%	67%
Cloud backup	5%	30%	65%
Auditing of user activity	5%	31%	64%
Review of access rights (attestation)	6%	34%	60%
Data classification	9%	44%	47%
Remove sensitive files from the cloud	18%	38%	44%
Cloud access security broker	20%	42%	38%

95% of large enterprises are auditing user activity in the cloud or plan to do so.

Cloud backup is the most commonly used protection measure among large organizations; only 5% of them do not already use or plan to use this option.

Medium (101-1,000 employees)

	NOT GOING TO DO	PLAN TO DO	ALREADY DO
Multifactor authentication	7%	28%	65%
Employee trainings	7%	31%	62%
Encryption	6%	35%	59%
Cloud backup	7%	38%	55%
Auditing of user activity	5%	43%	52%
Review of access rights (attestation)	8%	43%	49%
Data classification	17%	54%	28%
Remove sensitive files from the cloud	33%	43%	24%
Cloud access security broker	32%	51%	17%

Small (1-100 employees)

	NOT GOING TO DO	PLAN TO DO	ALREADY DO
Multifactor authentication	9%	26%	65%
Employee trainings	9%	28%	63%
Encryption	12%	32%	56%
Cloud backup	11%	34%	55%
Auditing of user activity	12%	34%	54%
Review of access rights (attestation)	11%	36%	53%
Data classification	26%	40%	34%
Remove sensitive files from the cloud	39%	30%	31%
Cloud access security broker	40%	45%	15%

UNCLOUDING

The most resolute way of securing data in the cloud is to remove it from the cloud. In 2019, 48% of respondents had moved or were planning to move sensitive data back on premises. In 2020, despite the surge in cloud adoption due to the need to support remote work, this figure increased to 62%. This year, it grew to 66%.

66%

of organizations has already removed sensitive data from the cloud or plan to do so

Paradoxically, 78% of respondents are satisfied with their organization's cloud security— but 66% have already moved sensitive data back on premises or plan to do so. Plus, 20% of organizations simply don't store any sensitive information in the cloud. This indicates that organizations believe their data is safer when it's on premises. One reason is that cloud solutions are newer and therefore less mature, and many security concerns are out of cloud provider's scope of responsibilities, which makes cloud expertise within the internal IT team crucial. Of course, on-premises servers are not invulnerable, so organizations need to find the right balance between security and the business need for having data available in the cloud.

Dirk Schrader

VP of Security Research at Netwrix

IMPACT OF SECURITY MEASURES ON DETECTION TIME

Data classification enables organizations to tag sensitive files so they can improve their control over where data is stored and who can access it. This technology significantly improved the speed of discovery for all types of incidents: The majority of respondents who classify their data were able to detect an attack within minutes, while those who don't classify data usually needed hours or even days.

IMPACT OF DATA CLASSIFICATION ON SPEED OF INCIDENT DETECTION

	CLASSIFY DATA	DON'T CLASSIFY DATA
Phishing	48% discovered in minutes	41% discovered in hours
Ransomware or other malware attack	46% discovered in minutes	42% discovered in hours
Targeted attacks on cloud infrastructure	44% discovered in minutes	46% discovered in hours
Account compromise	39% discovered in minutes	35% discovered in hours
Data loss	37% discovered in minutes	37% discovered in hours
Accidental data leakage	32% discovered in minutes	31% discovered in hours
Data theft by hackers	32% discovered in minutes	31% discovered in hours
Data theft by insiders	29% discovered in minutes	30% discovered in days
Supply chain compromise	29% discovered in minutes	29% discovered in hours

IMPACT OF AUDITING OF USER ACTIVITY ON SPEED OF INCIDENT DETECTION

Auditing of user activity turned out to be a great way to improve the speed of incident detection. It was particularly effective for phishing, ransomware attacks and account compromise, where it reduced detection time from hours to minutes.

	AUDIT USER ACTIVITY	DON'T AUDIT USER ACTIVITY
Phishing	49% discovered in minutes	45% discovered in hours
Ransomware or other malware attack	41% discovered in minutes	43% discovered in hours
Targeted attacks on cloud infrastructure	35% discovered in minutes	35% discovered in hours
Account compromise	36% discovered in minutes	23% discovered in minutes
Data loss	30% discovered in minutes	18% discovered in minutes
Accidental data leakage	26% discovered in minutes	17% discovered in minutes
Data theft by hackers	26% discovered in minutes	17% discovered in minutes
Data theft by insiders	23% discovered in minutes	15% discovered in minutes
Supply chain compromise	23% discovered in minutes	26% discovered in minutes

CLOUD SECURITY CHALLENGES

The top 3 data security challenges named by survey respondents stayed the same from 2020: lack of IT staff, lack of expertise in cloud environments and lack of budget.

Most organizations accepted the new reality of remote work and adjusted their business processes to pandemic conditions. As a result, 33% of respondents now name IT staffing issues and lack of cloud expertise as the biggest cloud security challenges.

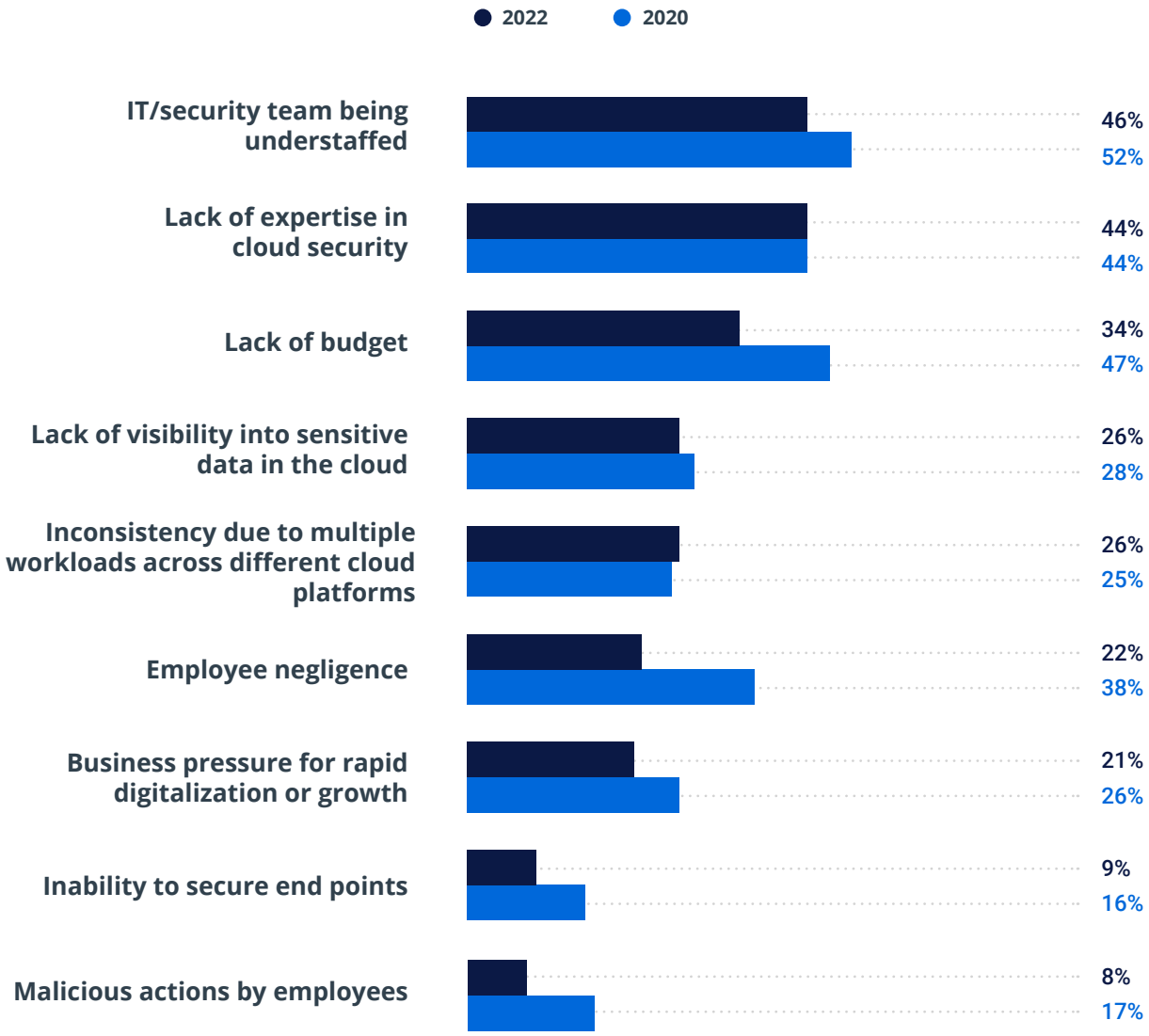
Dirk Schrader

VP of Security Research at Netwrix

While lack of budget is still in the top 3, the share of those who struggle with this problem dropped from 47% in 2020 to 34% in 2022 — budgets are increasing, and IT teams are learning how to allocate the money effectively. Employee negligence is challenging for 22% of respondents, down from 38% in 2020. Cybersecurity awareness is rising thanks to increased training and constant reminders about not opening suspicious links in emails allegedly from company's CEO.

Dirk Schrader

VP of Security Research at Netwrix



In 2020, 48% of CISOs noted that the business's desire for growth hinders efforts to ensure data security in the cloud. Now, this problem was named by only 20% of CIOs and 23% of CISOs.

BUDGETING

IT teams have also had to adjust their budgets to meet the needs of their remote or hybrid workforce. In 2020, organizations allocated 27% of their total cybersecurity budget to cloud security. In 2022, this share rose to 32% overall, and to 36% among large companies (1,000+ employees).

With 54% of workloads expected to be in the cloud by 2023, security budgets are growing. 49% of our respondents say their budget for cloud security increased in 2022.

In 56% of large organizations (1,000+ employees), the cloud security budget increased in 2022.

"The growing share of money spent on cloud security within the overall security budget shows the increasing importance of the cloud infrastructure within the IT environments of organizations. As the percentage of the cloud budget went up, it means something else had to go down as cloud safety became a higher priority. This will be a crucial balancing act for most organizations in the coming years" said Dirk Schrader, VP of Security Research at Netwrix.

Portion of cybersecurity budget allocated to cloud security (Average Number)

APPENDIX 1:

GEOGRAPHY

UNITED KINGDOM

88% of UK organisations store sensitive data in the cloud.

Top 3 types of sensitive data UK organisations store in the cloud

Personally Identifiable Information (PII) of customers	65%
Personally Identifiable Information (PII) of employees	42%
Corporate financial information	31%

What percentage of your workloads are in the cloud today?

53%

What percentage of your workloads are planned to be in the cloud in 12–18 months?

69%

Top 3 primary cloud adoption goals in the UK

84%	Reduce costs
64%	Improve security
48%	Organize infrastructure for remote workers

65% of UK respondents named integration with existing IT environment as a main factor that slows down cloud adoption in their organisations.

The biggest challenges UK organizations face while trying to ensure data security in the cloud

IT/security team being understaffed	46%
Lack of expertise in cloud security	46%
Lack of budget	46%

Most common cybersecurity incidents in the UK

Phishing	69%
Account compromise	35%
Targeted attacks on cloud infrastructure	31%

52% of the UK organisations experienced cyber attacks on their cloud infrastructure in the past 12 months

Time to detect incidents in the cloud

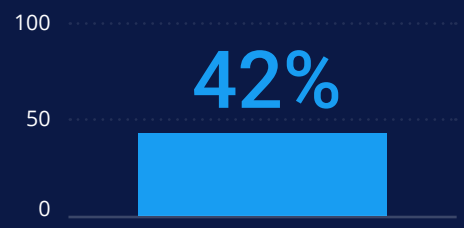
	MINUTES	HOURS	DAYS	WEEKS	MONTHS AND MORE
Phishing	61%	22%	13%	0%	4%
Ransomware or other malware attack	48%	31%	13%	4%	4%
Targeted attacks on cloud infrastructure	39%	35%	9%	9%	8%

22% of UK organisations needed weeks to detect data theft by hackers, and 17% needed months and more to detect supply chain compromise.

Top 3 measures UK organizations already take to protect data in the cloud

91%	Multifactor authentication
82%	Encryption
77%	Review of access rights (attestation)/ Cloud backup

Cybersecurity budget distribution



36% of UK organisations plan to implement data classification to better protect data in the cloud

FRANCE

73% of French organizations store sensitive data in the cloud.

Top 3 types of sensitive data French organizations store in the cloud

Personally Identifiable Information (PII) of employees	47%
Personally Identifiable Information (PII) of customers	33%
Corporate financial information	27%

What percentage of your workloads are in the cloud today?

37%

What percentage of your workloads are planned to be in the cloud in 12–18 months?

51%

Top 3 primary cloud adoption goals in France

Reduce costs	71%
Improve security	36%
Organize infrastructure for remote workers	29%

64% of French respondents named integration with existing IT environment as a main factor that slows down cloud adoption in their organizations.

The biggest challenges French organizations face while trying to ensure data security in the cloud

53%	Lack of expertise in cloud security
40%	IT/security team being understaffed
33%	Lack of visibility into sensitive data in the cloud

54% of French organizations experienced cyber attacks on their cloud infrastructure in the past 12 months.

Most common cybersecurity incidents in France

87%	Phishing
33%	Account compromise
33%	Accidental data leakage

Time to detect incidents in the cloud

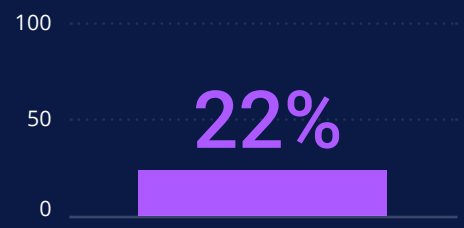
	MINUTES	HOURS	DAYS	WEEKS	MONTHS AND MORE
Phishing	38%	31%	23%	8%	0%
Ransomware or other malware attack	23%	38%	23%	0%	16%
Targeted attacks on cloud infrastructure	15%	38%	38%	0%	9%

46% of French organizations needed weeks to detect data theft by insiders, and 23% needed months and more to detect supply chain compromise.

Top 3 measures French organizations already take to protect data in the cloud

91%	Multifactor authentication
82%	Encryption
77%	Review of access rights (attestation)/ Cloud backup

Cybersecurity budget distribution



38% of French organizations plan to implement user activity audit to better protect data in the cloud

APPENDIX 2:

VERTICALS

MANUFACTURING

88% of manufacturing organizations store sensitive data in the cloud. The most common type (43%) is corporate financial information.

Top 3 primary cloud adoption goals

Organize infrastructure for remote workers	57%
Improve security	54%
Reduce costs	50%

What percentage of your workloads are in the cloud today?

35%

What percentage of your workloads are planned to be in the cloud in 12–18 months?

52%

Lack of budget is the main factor that slows down cloud adoption for 45% of respondents comparing to 35% on average.

The biggest challenges manufacturing organizations face while trying to ensure data security in the cloud

45%	Lack of budget
38%	Lack of expertise in cloud security
34%	IT/security team being understaffed

Manufacturing organizations suffered from some types of attacks more often than others within the last 12 months.

38% of respondents in this sector had to deal with account compromise at least once comparing to 31% on average.

Manufacturing is also more prone to supply chain compromise:

19% of organizations in this sector experienced this type of attack while the average number is 15%.

Time to detect incidents in the cloud

	MINUTES	HOURS	DAYS	WEEKS	MONTHS AND MORE
Ransomware or other malware attack	36%	40%	20%	0%	4%
Phishing	45%	40%	13%	0%	2%
Account compromise	23%	49%	21%	3%	4%

38% of manufacturing organizations needed days to detect data theft by hackers.

48% consider their own business employees as one of the biggest risks to data security in the cloud while the average number is 39%.

Top 3 measures financial organizations already take to protect data in the cloud

75%	Multifactor authentication
70%	Auditing of user activity
66%	Cloud backup

45% of respondents plan to implement data classification as a protective measure.

41% of manufacturing organizations plan to add access reviews and employee trainings to their cybersecurity bucket.

EDUCATION

83% of educational organizations store sensitive data in the cloud.

Top 3 types of sensitive data educational organizations store in the cloud

Personally Identifiable Information (PII) of customers	65%
Personally Identifiable Information (PII) of employees	54%
Corporate financial information	25%

What percentage of your workloads are in the cloud today?

44%

What percentage of your workloads are planned to be in the cloud in 12–18 months?

56%

Top 3 primary cloud adoption goals

79%	Reduce costs
65%	Improve security
52%	Organize infrastructure for remote workers

44% of respondents define integration with existing IT environment as a main factor that slows down cloud adoption in their organizations.

The biggest challenges educational organizations face while trying to ensure data security in the cloud

50%	IT/security team being understaffed
46%	Lack of expertise in cloud security
38%	Employee negligence

47%

of educational organizations experienced a cyber attack on their cloud infrastructure within the last 12 months.

Educational sector is 11% more likely to face account compromise:

42%

of respondents experienced this kind of attack compared to the average of 31% from the other industries surveyed.

Time to detect incidents in the cloud

	MINUTES	HOURS	DAYS	WEEKS	MONTHS AND MORE
Ransomware or other malware attack	30%	37%	27%	2%	4%
Phishing	35%	46%	15%	4%	0%
Account compromise	22%	41%	30%	5%	2%

20%

of educational organizations needed weeks to detect data theft by hackers.

27%

of respondents say that incidents in the cloud lead to unplanned expenses to fix security gaps.

Educational organizations are more concerned about their own employees:

48% consider their staff to pose the biggest risk to data security in the cloud comparing to 39% on average.

Top 3 measures educational organizations already take to protect data in the cloud

75%	Multifactor authentication
73%	Employee trainings
68%	Cloud backup

32%

of respondents plan to implement access rights review as a protective measure in the cloud.

37%

of respondents say that their cloud security budget increased in 2022.

HEALTHCARE

73% of healthcare organizations store sensitive data in the cloud. The most common type (45%) is patient or protected health information.

Top 3 primary cloud adoption goals

Reduce costs	69%
Improve security	55%
Organize infrastructure for remote workers	33%

What percentage of your workloads are in the cloud today?

What percentage of your workloads are planned to be in the cloud in 12–18 months?

59% of respondents say integration with existing IT environment is the main obstacle for faster cloud adoption compared to 41% among the other industries.

The biggest challenges healthcare organizations face while trying to ensure data security in the cloud

69%	IT/security team being understaffed
55%	Lack of expertise in cloud security
33%	Lack of budget

61% of respondents experienced an attack on their cloud infrastructure within the last 12 months. The most common cloud security incidents were phishing, ransomware or other malware attack and targeted attack on cloud infrastructure.

Time to detect incidents in the cloud

	MINUTES	HOURS	DAYS	WEEKS	MONTHS AND MORE
Ransomware or other malware attack	29%	47%	22%	2%	0%
Phishing	40%	40%	18%	2%	0%
Account compromise	24%	45%	20%	7%	4%

ONLY

14%

of those who experienced an attack say it had no impact on their organization compared to **32%** among all other verticals surveyed.

48%

consider contractors and partners with legitimate access as the biggest risk to data security in the cloud.

Top 3 measures healthcare organizations already take to protect data in the cloud

73%	Encryption
66%	Multifactor authentication
61%	Employee training

64%

of respondents intend to implement data classification as a protective measure in the cloud.

43%

of healthcare organizations plan to add access reviews to their cloud security bucket.

FINANCE

80% of financial organizations store sensitive data in the cloud. The most common type (57%) is personally identifiable information of employees.

Top 3 primary cloud adoption goals

Reduce costs	62%
Improve security	58%
Increase responsiveness to customer needs	46%

What percentage of your workloads are in the cloud today?

What percentage of your workloads are planned to be in the cloud in 12–18 months?

46% of respondents name regulatory compliance as a factor that slows down cloud adoption in their organization compared to only 30% among other verticals surveyed.

The biggest challenges financial organizations face while trying to ensure data security in the cloud

51%	Lack of expertise in cloud security
45%	IT/security team being understaffed
45%	Lack of visibility into sensitive data in the cloud

61% of respondents experienced an attack on their cloud infrastructure within the last 12 months. The most common cloud security incidents were phishing, ransomware or other malware attack and targeted attack on cloud infrastructure.

Time to detect incidents in the cloud

	MINUTES	HOURS	DAYS	WEEKS	MONTHS AND MORE
Phishing	42%	49%	7%	2%	0%
Accidental data leakage	25%	33%	25%	13%	4%
Ransomware or other malware attack	38%	40%	20%	2%	0%

74%

of respondents experienced phishing within the last 12 months which makes this kind of attack the most common for this vertical.

48%

of financial institutions faced accidental data leakage compared to 25% among other industries surveyed.

Top 3 measures financial organizations already take to protect data in the cloud

80%	Multifactor authentication
78%	Encryption
78%	Cloud Backup

47%

of respondents plan to implement data classification as a protective measure in the cloud.

22%

are aimed at improving their cybersecurity posture through the regular attestation of access rights.

GOVERNMENT

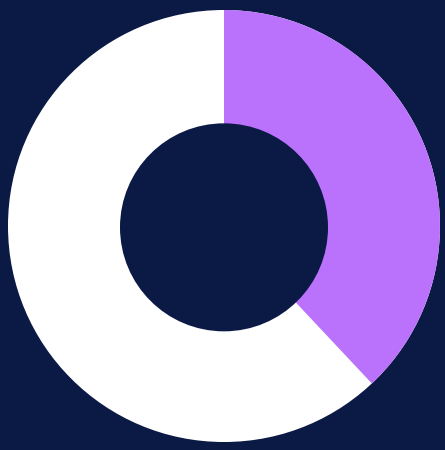
39% of government agencies do not store sensitive data in the cloud compared to only 20% among other verticals surveyed.

Top 3 primary cloud adoption goals

Improve security	57%
Reduce costs	49%
Organize infrastructure for remote workers	43%

What percentage of your workloads are in the cloud today?

What percentage of your workloads are planned to be in the cloud in 12–18 months?



Regulatory compliance and higher level of security risks mainly slow down cloud adoption for 45% and 44% of governments institutions, respectively, while only 30% of respondents from other verticals define these reasons as main factors.

The biggest challenges governmental organizations face while trying to ensure data security in the cloud

56%	Lack of expertise in cloud security
52%	IT/security team being understaffed
52%	Lack of budget

Every third governmental institution (35%) experienced an attack on their cloud infrastructure within the last 12 months.

Time to detect incidents in the cloud

	MINUTES	HOURS	DAYS	WEEKS	MONTHS AND MORE
Phishing	34%	45%	15%	2%	4%
Ransomware or other malware attack	34%	38%	17%	2%	9%
Data loss	21%	43%	23%	4%	9%

15%

of governmental agencies needed months and more to detect data theft by hackers compared to 9% among other verticals surveyed.

47%

of respondents are concerned about the risks associated with their own employees and consider this factor as the biggest risk to data security in the cloud.

Top 3 measures financial organizations already take to protect data in the cloud

60%	Multifactor authentication
60%	Encryption
56%	Cloud Backup

56%

of respondents plan to implement review of access rights as a protective measure in the cloud.

44%

of governmental institutions plan to add data classification to their cloud security bucket.

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/go/research

ABOUT NETWRIX

Netwrix makes data security easy by simplifying how professionals control sensitive, regulated and business-critical data, regardless of where it resides. More than 11,500 organizations worldwide rely on Netwrix solutions to secure sensitive data, realize the full business value of enterprise content, pass compliance audits with less effort and expense, and increase the productivity of IT teams and knowledge workers.

Founded in 2006, Netwrix has earned more than 150 industry awards and been named to both the Inc. 5000 and Deloitte Technology Fast 500 lists of the fastest growing companies in the U.S.

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