netwrix

2020

DATA RISK & SECURITY REPORT

www.netwrix.com

EXECUTIVE SUMMARY

Organizations are investing more than ever in cybersecurity, yet data breaches and other security incidents are continuing to increase in both number and size. Our survey identified several key factors that can help account for this. First, while security professionals successfully mitigate security issues at some of the six stages of data lifecycle, they often overlook other stages, leaving their organization's content vulnerable. In addition, security professionals generally know very little about what data they have, how sensitive it is, where it is stored, and who has access to it. Without deep visibility into internal processes and user activity, they struggle to answer the four foundational questions of security: Who? What? When? Where? Until they gain a deeper understanding into how data lives during all stages of its lifecycle, it will keep slipping through their fingers.

The data storage stage turned out to be the most challenging stage for ensuring data protection. Nearly a quarter (24%) of organizations reported they had discovered data outside of secure locations, and it took them days (43%) or weeks (23%) to discover the incident. These figures represent the highest incident rate and the slowest detection time of all the stages.

Other notable findings of the report include:

61%

of organizations that are subject to the GDPR collect more customer data than the law permits.

100%

of organizations that have hired a chief data officer (CDO) have implemented data discovery and classification processes.

91%

of organizations claim they store sensitive and regulated data only in secure locations, but 24% of them admitted they had discovered such data outside of designated locations in the past year.

54%

of organizations said that they do not follow the security best practice of reviewing user access rights to data on a regular basis.

30%

of system administrators granted direct access to sensitive and regulated data based only on a user request in the past 12 months.

66%

of CIOs don't have cybersecurity and risk KPIs that are regularly reported to their executives.

Organizations that classify data at creation spend just an average of 3 hours on each data subject access request (DSAR) — 11 times faster than those who don't classify their data. In addition, they said their cost for managing DSARs increased by 24% or less, while those who don't classify data reported increases of 50%–74%.

46%

of organizations that had an unauthorized data sharing incident are subject to the GDPR. However, 38% of them are confident that employees don't bypass IT control to share data.

7%

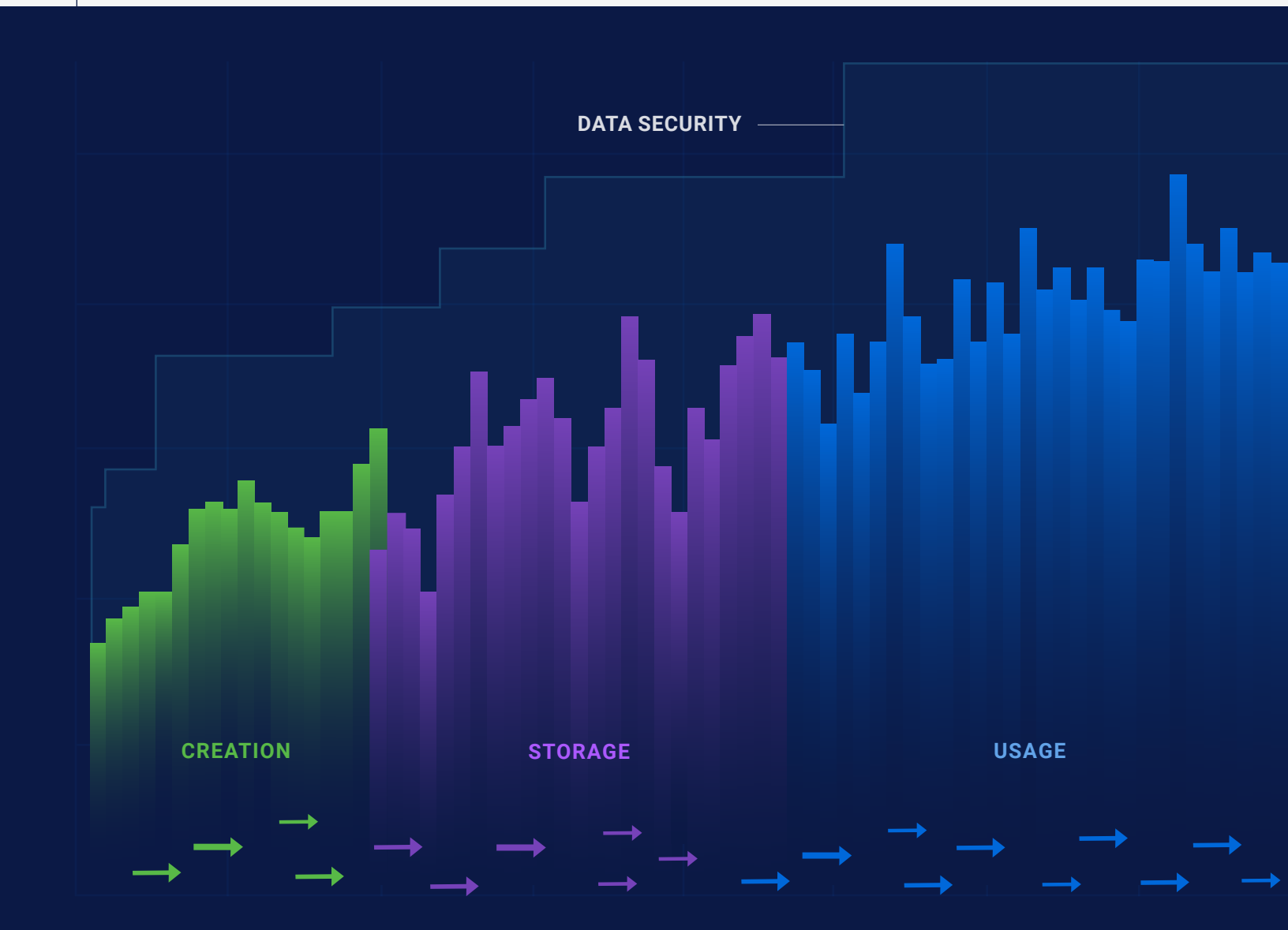
of organizations had security incidents during the data archival stage, but 58% of them noted that the data was compromised, which is the largest share among all the stages.

30%

of organizations that don't have data classification processes never get rid of redundant, obsolete and trivial (ROT) data, as opposed to just 6% of those who do classify their data.

HOW TO READ THIS SURVEY

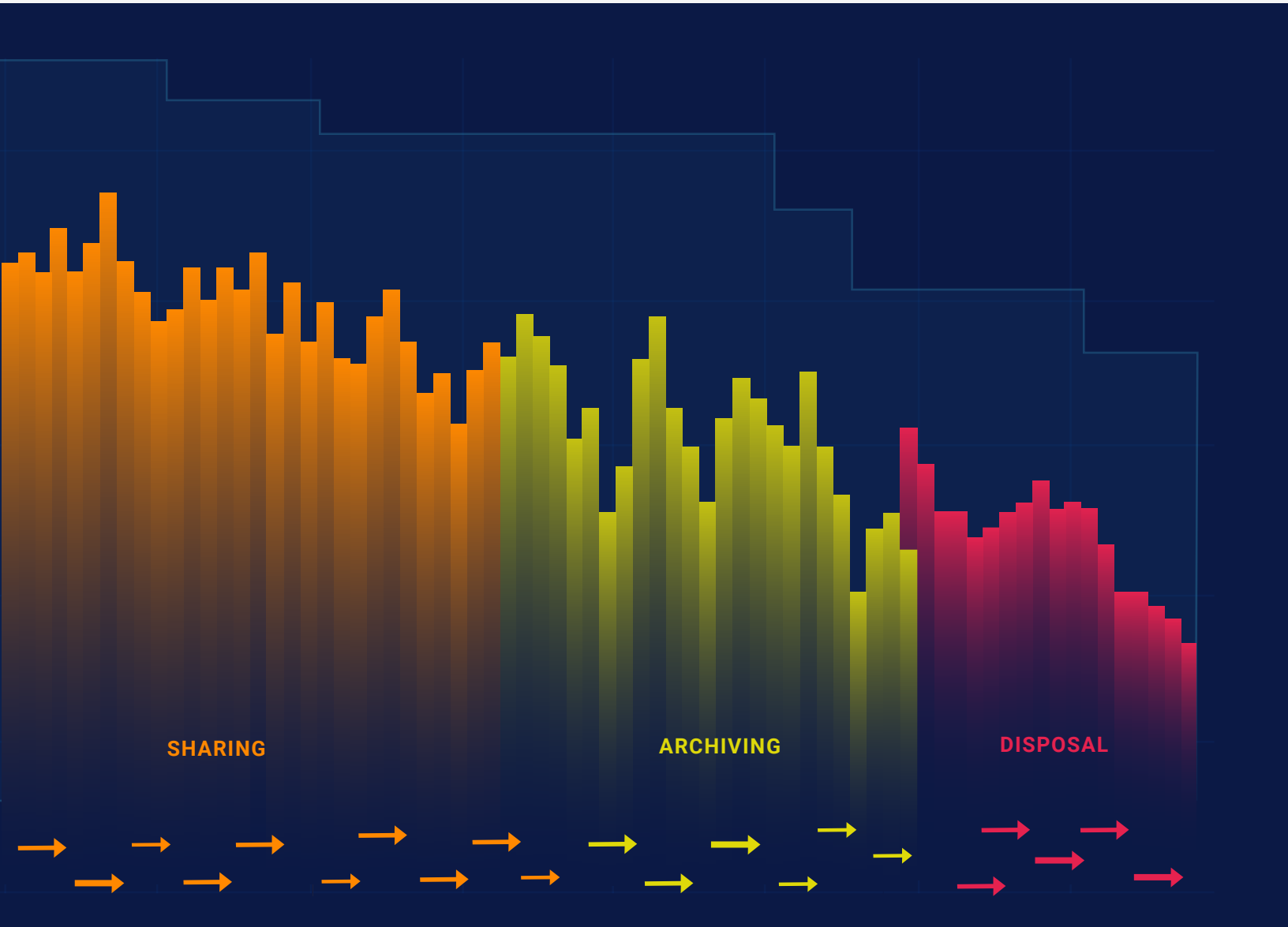
Pic. 1 Data lifecycle



In October 2019, Netwrix launched an online survey of IT professionals worldwide to find out how their organizations treat data during each stage of its lifecycle and to identify security gaps that can put sensitive or regulated data at risk. The survey included 53 multiple-choice questions that also allows respondents to supply own answers. Over the course of the month, we gathered insights from 1045 respondents; a detailed demography is provided at the end of this report.

The survey yielded a number of interesting findings, which are organized as follows: The main body of the document provides aggregated results across all respondents, regardless of vertical and location, for each of the six stages of the data lifecycle (creation, storage, usage, sharing, archival and disposal). The appendixes detail key results by vertical, macro region and micro region.

CREATION	Data first appears in the organization.
STORAGE	Data is placed for further usage.
USAGE	Data is being accessed and used by stakeholders.
SHARING	Data is being shared between stakeholders.
ARCHIVING	Data is placed for long-term
DISPOSAL	Data is identified as unneeded and deleted.



AGGREGATED RESULTS FOR ALL RESPONDENTS

STAGE 1:

DATA CREATION

The majority of organizations lack clear data collection policies. 64% of respondents said they couldn't confirm that their organizations gather and store only the minimum amount of customer data required. Of those, 34% are subject to the GDPR, and Article 25 of that law requires them to collect and process only the personal data that is necessary for each specific purpose.

In addition, 41% of respondents that are subject to the GDPR and 42% of those subject to the CCPA admitted that they are unable to discover and classify data at the point of creation, or are unaware that such a capability even exists. Both Article 30 of the European legislation and Section 1798.100 of the California law require organizations to track all personal data they gather and ensure that its storage and use is aligned with the stated purposes of data collection. Data classification provides IT security professionals with more context into their data landscape, so they can better prioritize their efforts and focus on the areas that contain the most critical information.

The majority of CIOs (71%) and CISOs (73%) surveyed consider poor visibility into what data is being created or acquired to be a cybersecurity and compliance risk. Nevertheless, 48% of CIOs and 43% of CISOs have no means of discovering sensitive data and tagging it by classification, or are unaware that such capabilities exist.

GDPR: Maintain records of processing activities

The text of the GDPR does not use the terms "data inventory" or "mapping," but these processes are essential to building a data security program that complies with the law. For example, data inventory is the first step in complying with Article 30, since it requires companies to **maintain detailed records** of their processing activities, including the purposes of the processing, the categories of data subjects and personal data, and any recipients with whom personal data is shared.

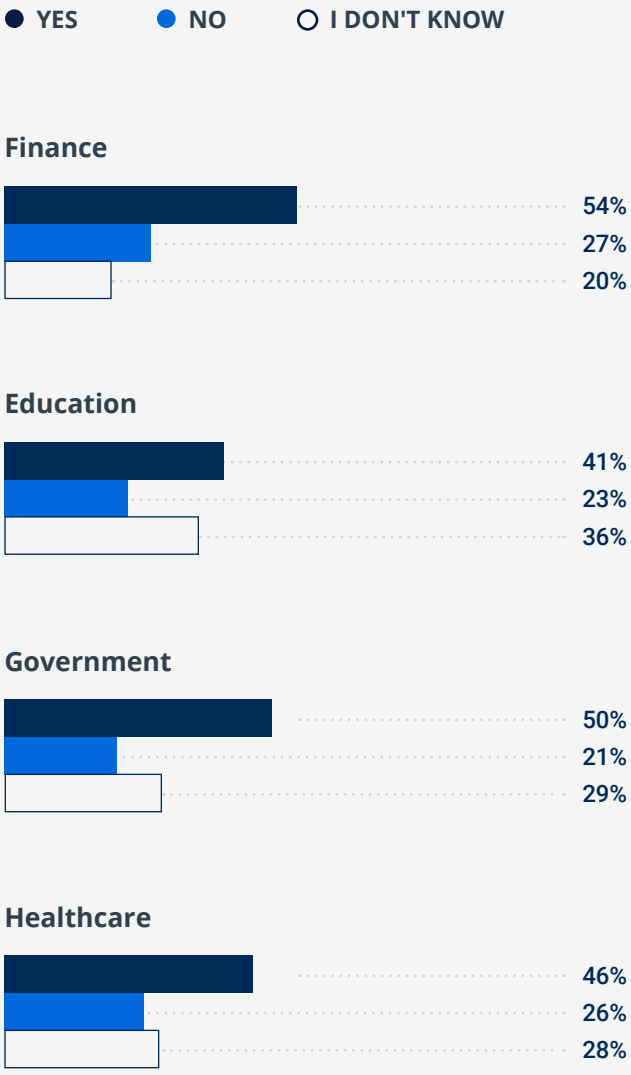
RECOMMENDATIONS

Work with senior management and data management teams to document the purposes of data collection and ensure that your organization gathers only the minimum amount of customer data to satisfy those needs. Automate data discovery and classification to ensure that the data you collect is handled according to your security policies and applicable compliance regulations.

CCPA:
Track data footprint

Although the CCPA does not explicitly mandate data inventory and records management, to comply with the law, organizations need to **track the footprint of personal information** of California consumers. In particular, they need effective data inventory to comply with Section 1798.100, which requires companies to disclose the categories of personal information they collect and the purposes of the data collection, and forbids them to use that data for additional purposes without notifying consumers.

Diagram 1. Has your organization adopted data discovery and classification technology?



100%

of organizations that have hired a chief data officer (CDO) have implemented data discovery and classification processes.

61%

of organizations that are subject to the GDPR collect more customer data than the law permits.

39%

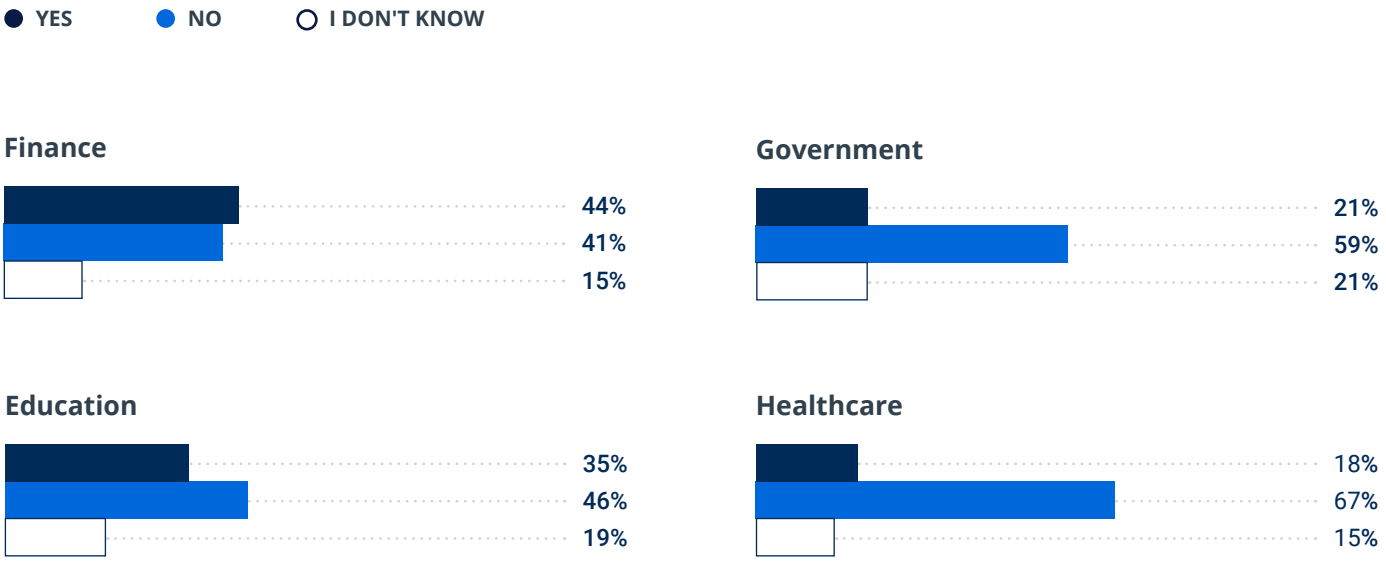
of respondents don't consider low visibility into data creation to be a security and compliance risk.

STAGE 2:

DATA STORAGE

The overwhelming majority of organizations (91%) claim they store sensitive and regulated data only in secure locations. However, this confidence is clearly misplaced, since 24% of them admitted discovering such data outside of designated secure locations in the past year — and in 62% of the cases, the data was left overexposed for days or even weeks. Moreover, about the same percentage of them reported that their IT staff granted direct access to sensitive and regulated data based solely on a user's request in the past year. Not surprisingly, 54% of these organizations suffered audit findings and fines for non-compliance.

Diagram 2. Did any of your system or IT administrators grant direct access rights based solely on a user's request in the past 12 months?

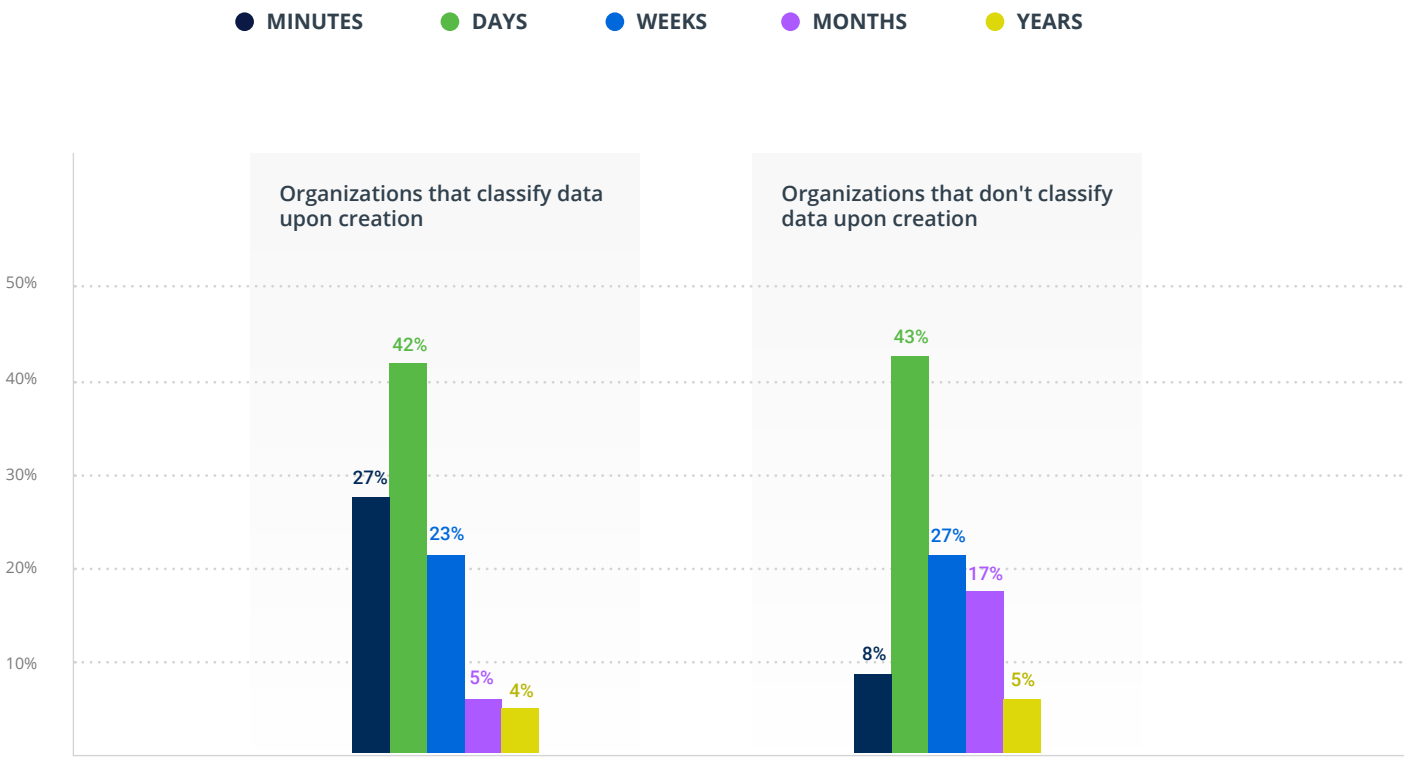


RECOMMENDATIONS

Make sure you are able to track where your sensitive and regulated data resides at any given time and that you are alerted if it surfaces in an improper location. Create approval workflows for granting data access rights, and ensure that you always know if a user has been granted direct permissions to critical data.

Data storage proved to be the most problematic stage in terms of risk mitigation. It took many organizations days (43%) or weeks (23%) to detect data outside of secure locations (which, as we will see, is much slower than the risk mitigation during other stages). Notably, organizations that classify their data upon creation are better able to spot improperly stored data in minutes (see Diagram 3).

Diagram 3. Average time to detect data outside of secure locations, based on use of data classification



66%

of CISOs and compliance officers are not sure if they store regulated data only in secure locations. Most of them work in organizations subject to PCI DSS (51%) and GDPR (45%).

30%

of system administrators granted direct access to sensitive and regulated data based only on a user request in the past year. This risk was most common in the financial (44%) and education (35%) sectors.

None

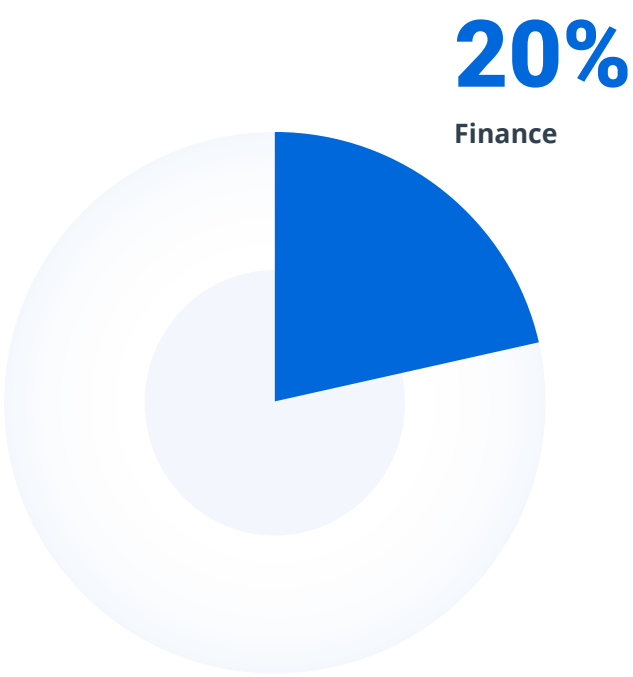
of the educational organizations surveyed said they could to detect data outside of a secure location in minutes.

STAGE 3:

DATA USAGE

More than half of organizations (54%) admitted that they do not follow the security best practice of reviewing user access rights to data on the regular basis. Specifically, 38% of respondents said they review access rights occasionally and 16% do it rarely or never. Not surprisingly, 38% of these organizations suffered a data breach in the past 12 months. The top verticals breached were the financial sector (20%) and the software industry (17%).

Diagram 4. Percentage of organizations that experienced a data breach due to data misuse in the past 12 months, by industry



Overall, organizations report that it typically takes them days (49%), minutes (22%) or even weeks (21%) to detect data misuse, such as use of data for purposes outside the scope of initial data collection. Among those who detect such incidents in minutes, 85% classify data at the stage of creation.

HANDLING DATA SUBJECT REQUESTS

With regulations like the GDPR and the CCPA on the rise, handling data subject requests (DSARs) is becoming an increasingly important part of the data usage stage. Only 21% of CISOs responsible for GDPR compliance said their organizations did not see a rise in DSARs during the past 12 months. However, 26% of them found it difficult to evaluate whether they had more requests than last year.

The most time-consuming and labor-intensive part of responding to a DSAR is gathering the relevant data. Classifying data in categories and ensuring fast search helps IT teams complete the job faster and with less effort. Most organizations need hours (80%) or even days (11%) to deal with each DSAR, but organizations that classify data at creation and are able to search through it spend just an average of 3 hours on each DSAR —11 times faster than those who don't classify their data.

In addition, CISOs at organizations that classify data say that the costs for managing DSARs increased by 24% or less, while those who don't classify data reported increases of 50%–74%.

Diagram 5. Average time (hours) spent on each DSAR request, by industry and use of data classification

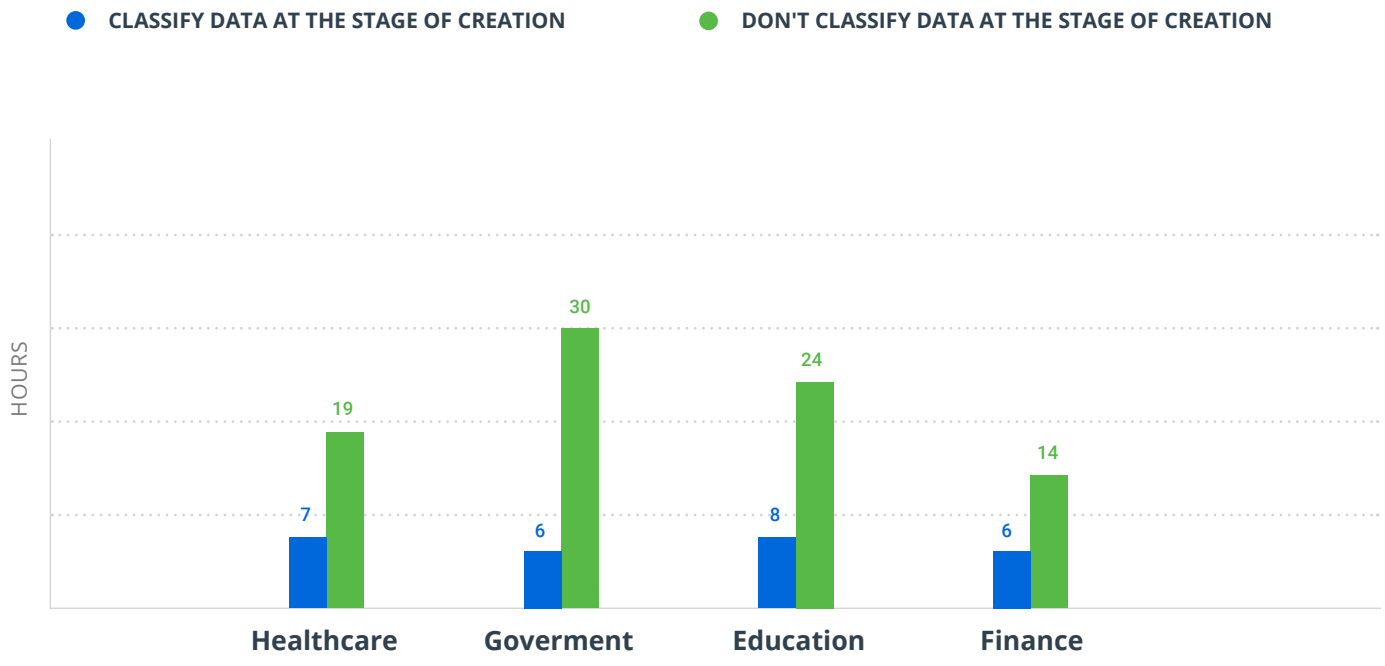
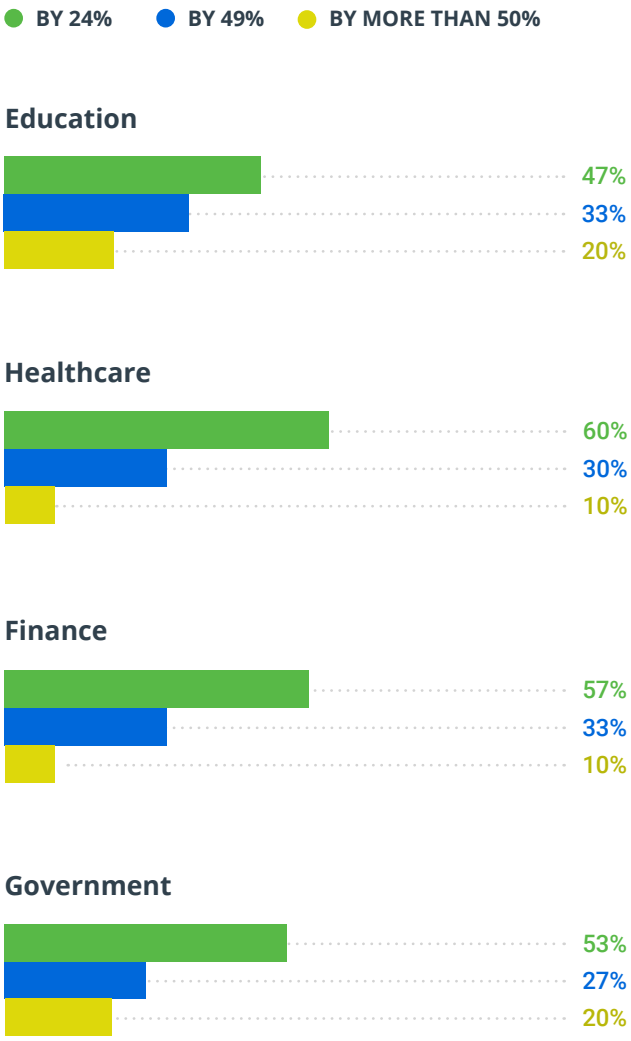


Diagram 6. Average increase in cost of DSAR management, by industry



RECOMMENDATIONS

Regularly conduct entitlement reviews to minimize the risk of user misuse. If your organization is subject to privacy legislation, streamline the processing of DSARs by ensuring you are able to search through your data to identify all information related to a particular data subject.

18%

of CISOs reported misuse of sensitive data in their organizations during the past 12 months; in 38% of those cases, the data was compromised.

31%

of organizations that are subject to the GDPR but don't classify their data say that it takes them months to detect security incidents related to data usage.

33%

of government and 29% of financial organizations noticed an increase in DSAR requests during the previous year.

5 min is the shortest time needed to comply with a single data subject request.

2 months is the longest time need to satisfy each DSAR. (Note that regulations often require a response within one month.)

STAGE 4:

DATA SHARING

About half of organizations (54%) are confident that their employees are not sharing data using any means of communication unknown to the IT team. Unfortunately, most of them can't prove it, since 29% of them don't track employee data sharing at all, and another 25% have only error-prone manual processes for tracking. Even though modern privacy regulations require companies to track the footprint of the personal data they collect, 33% of organizations subject to the GDPR and 25% of those subject to the CCPA do not track data sharing at all.

Just 12% of organizations reported a security incident due to unauthorized data sharing during the previous year. Of those, 55% of respondents needed days to discover it, and 44% confirmed that the incident resulted in a data breach. Organizations with automated processes to monitor data sharing were able to detect incidents sooner; 48% of them spotted the incident in minutes, something only 7% of those using manual processes achieved.

RECOMMENDATIONS

Educate your employees about secure data-sharing techniques and explain the consequences of unauthorized data sharing. However, do not rely on users to always do the right thing; automate monitoring of user activity to know if sensitive data is mishandled.

Diagram 7. Does your organization track data sharing among employees?

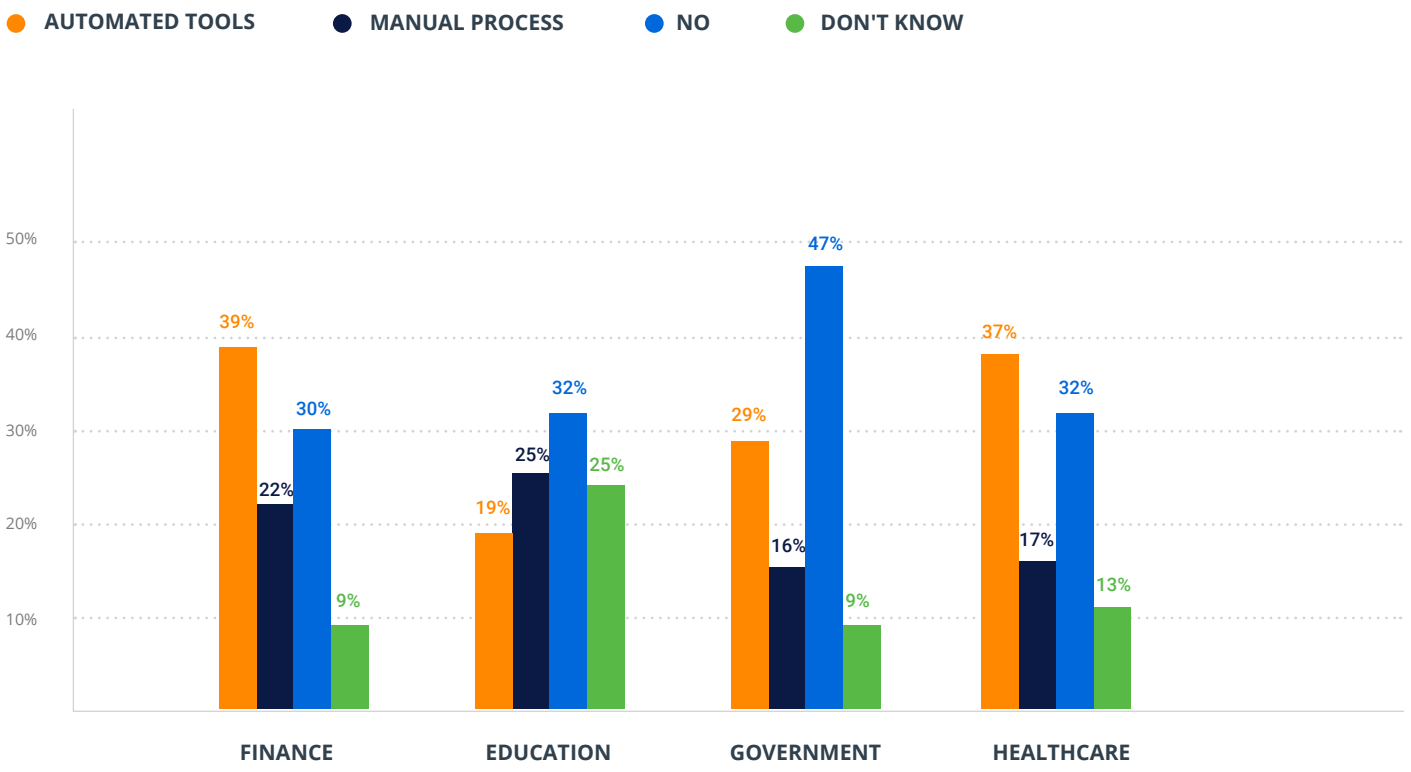
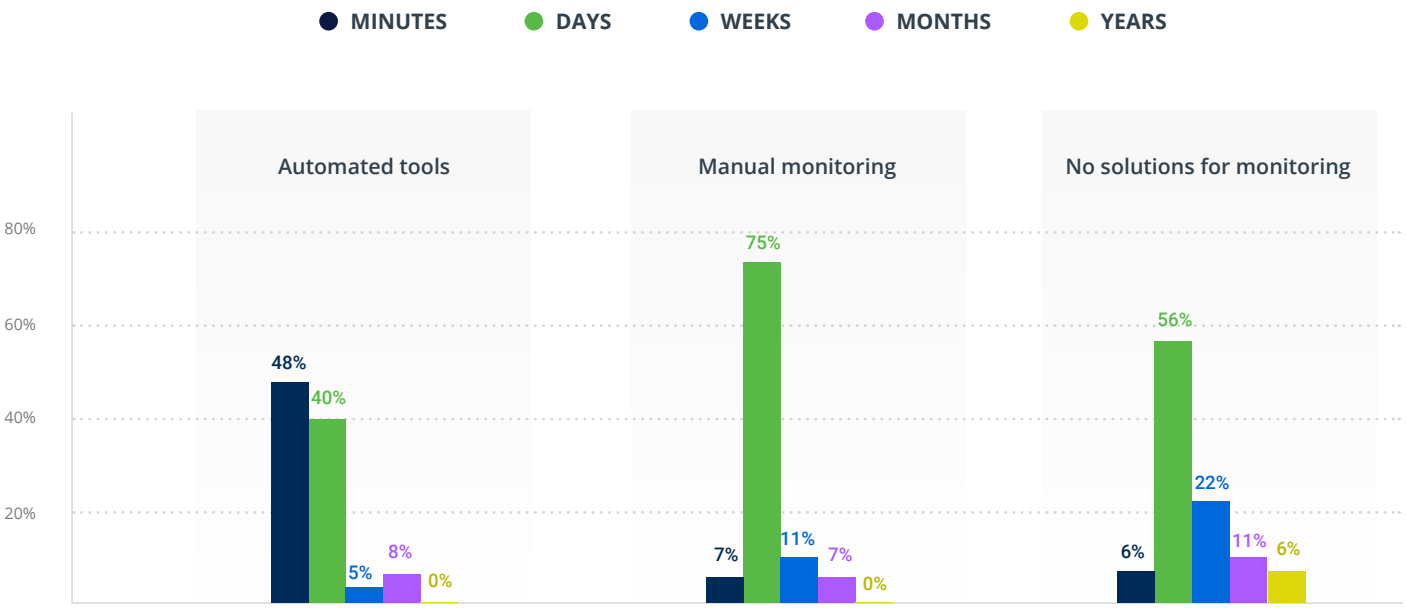


Diagram 8. Average time needed to detect data sharing incidents, based on monitoring method



STAGE 5:

DATA ARCHIVAL

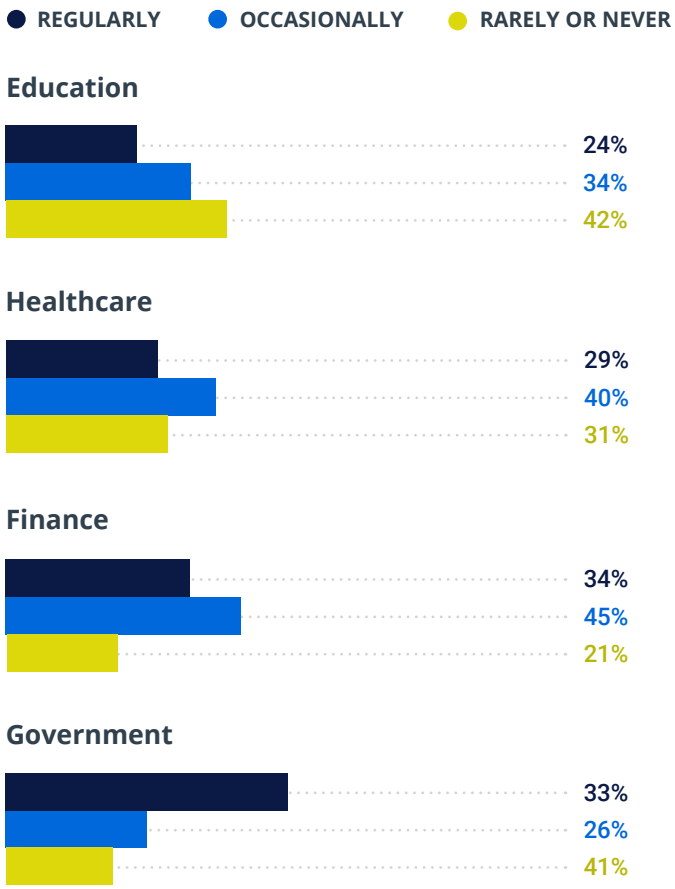
Most organizations treat their archived data even worse than their active data. In particular, 74% of respondents admitted that they do not review access rights to their archived data on a regular basis; 41% review them occasionally and 33% do it rarely or never. Of course, lack of strict access controls has a negative impact on data security: Among those who don't check access rights to archived data regularly, 52% reported a compromise of that data during the past 12 months.

Most organizations need days (38%) or weeks (28%) to detect security incidents involving archived data. However, data discovery and classification enables faster detection: As Diagram 10 shows, most organizations that have data classification in place spot incidents in minutes (24%) or days (43%), while those who don't classify their data need weeks (50%) or even months (13%).

RECOMMENDATIONS

Make sure that your archived data is protected similarly to your active data. Ensure that only a limited number of user accounts have access to it, and get alerts if the archived data is copied, modified or deleted.

Diagram 9. Frequency of access rights review for archived data, by vertical



75%

of CIOs and 71% of CISOs admit that permissions to archived data are not reviewed as regularly as they should be.

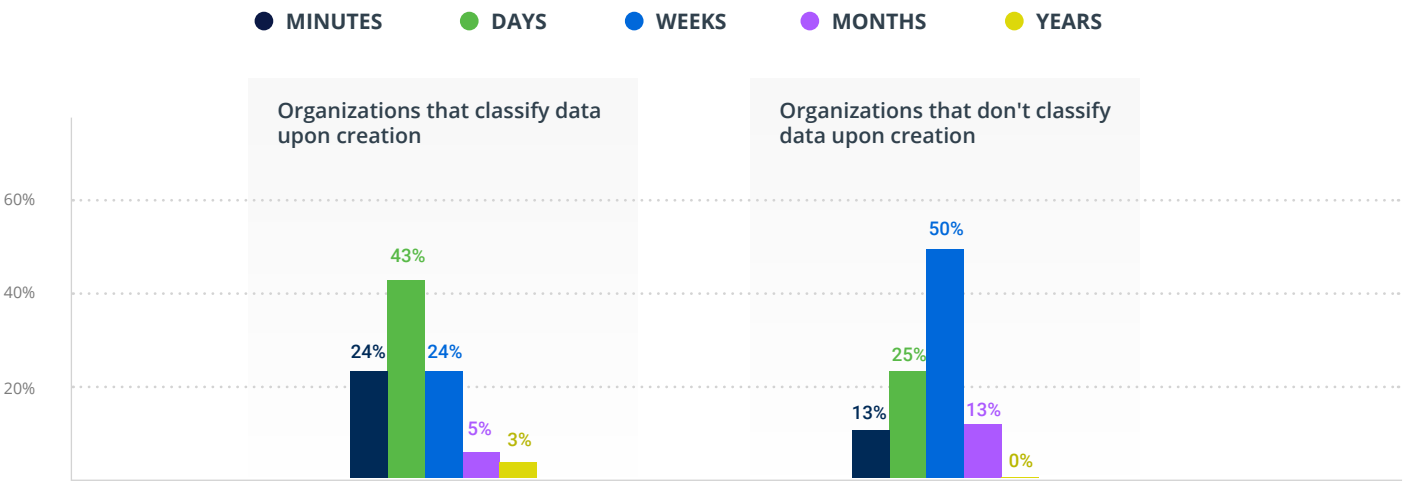
58%

of organizations that reported a security incident said that archived data was compromised.

48%

of organizations that suffered a data breach of archived data are subject to the GDPR and 24% are subject to the CCPA.

Diagram 10. Time required to detect security incidents involving archived data, based on use of data classification



STAGE 6:

DATA DISPOSAL

Data isn't just growing; it's exploding. Continuously removing unnecessary files is critical to achieving multiple goals, including:

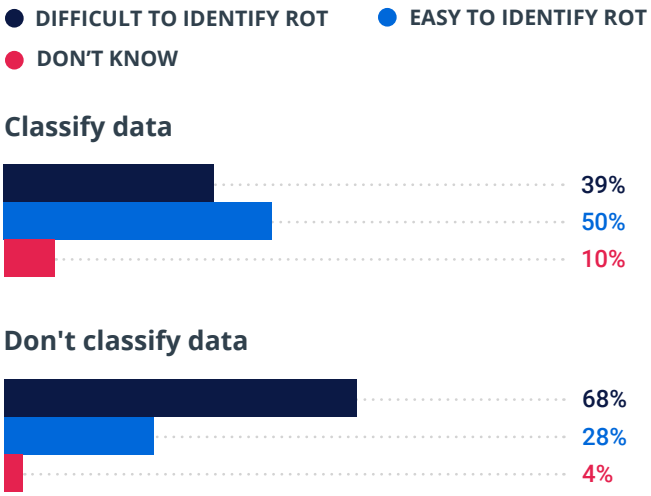
- Controlling storage and management costs
- Complying with regulations that have specific disposal requirements
- Addressing data access requests within the required time period
- Reducing potential attack surface

However, the vast majority of organizations lack a systematic approach to data destruction. In fact, more than half of the organizations surveyed (53%) have not yet implemented any data retention program, which means they cannot manage their records in line with legal obligations and company guidelines. Not surprisingly, 17% of them have mistakenly deleted necessary sensitive or regulated data in the past 12 months. In addition, only 29% of organizations say they regularly or continuously get rid of redundant, obsolete or trivial (ROT) data.

Not all compliance regulations impose data retention obligations. However, broad new privacy laws like the GDPR require organizations to discard regulated data that is no longer needed in a timely fashion. However, 52% of organizations that are subject to the GDPR still haven't established retention program as required by Article 25.

Organizations that have yet to adopt a continuous data classification process find it challenging to create and enforce retention policies. The majority of respondents (68%) have not implemented a retention program and do not classify their data. It is no wonder that 75% of them struggle to quickly and accurately identify ROT data. On the other hand, the 56% of organizations that do classify their data report no difficulties with the identification and deletion of unnecessary information.

Diagram 11. How easy is it for you to identify ROT data?



GDPR: Minimize data retention

The GDPR stipulates that personal data may only be stored for as long as absolutely necessary (Article 25). It is also stated that 'time limits should be established by the controller for erasure or for a periodic review' to ensure that the period for which the personal data is stored is limited to a strict minimum (Recital 39).

CCPA: Consider business needs

Although the CCPA give consumers the right to request that a business delete their personal information, the business may refuse if it can provide a valid reason — and Section 1798.105(d) lists so many possible justifications that organizations don't really need to have a data retention policy to comply with the CCPA. However, security best practices recommend to reduce the amount of stored data to avoid unnecessary risk.

14%

of organizations subject to the GDPR have mistakenly deleted needed sensitive or regulated data in the past 12 months.

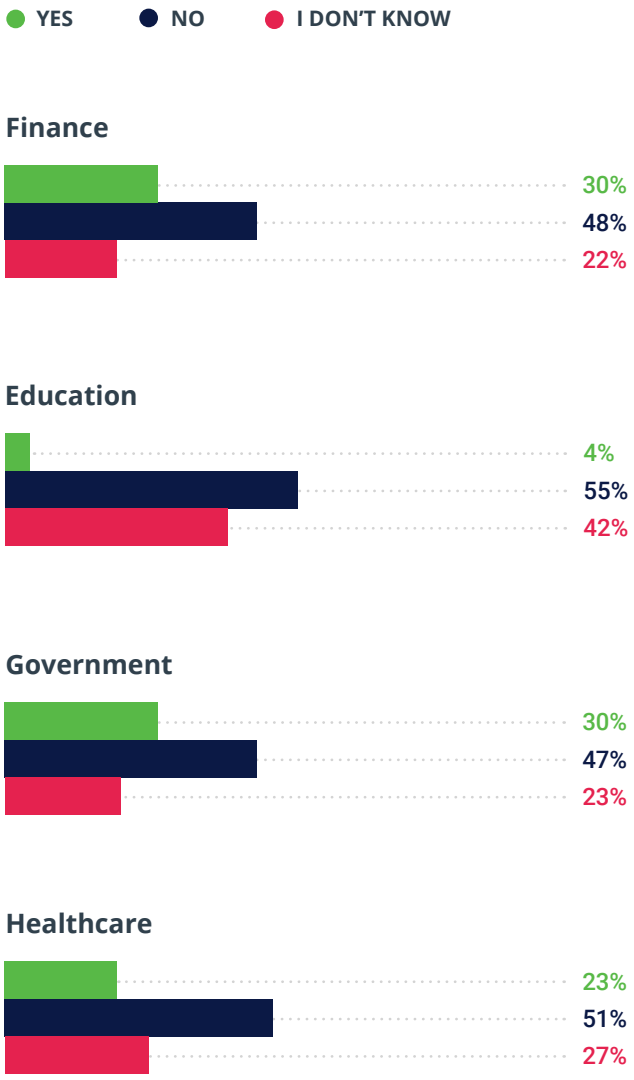
66%

of CIOs find it difficult to identify ROT data in their organizations.

30%

of organizations that don't have data classification processes never get rid of ROT data, as opposed to just 6% of those who do classify their data.

Diagram 12. Does your organization have a data retention program?



ONLY 4%

of educational institutions have implemented a data retention program. And 57% of educational organizations rarely or never purge their ROT data.

RECOMMENDATIONS

Establish a process for data disposal based on your business needs, legal and compliance requirements, and common sense. To reduce risks and control costs, make sure you can identify the data your organization no longer needs and remove it.

DATA RISK: REPORTING AND BUDGET

Less than half (48%) of cybersecurity professionals have security and risk KPIs that are regularly reported to management, and only 17% know how to measure the success of their cybersecurity initiatives. However, nearly a third (31%) of respondents said that their management now requests more reports on the state of data security than a year ago.

Among organizations that don't have any metrics to measure the efficiency of their data security programs, only 39% expect their IT budgets to grow, and only a third (34%) of them expect an increase of 25–49%. This is a disturbing finding, since these organizations will continue to be ill-prepared to evaluate the effectiveness of their data security efforts and demonstrate return on investment to business stakeholders. Organizations that have KPIs that they can communicate to the board of directors are more successful at getting budget increases (Diagram 14).

RECOMMENDATIONS

There is no standard list of cybersecurity metrics, so you should choose your KPIs based on your organization's needs. Make sure they are clear and easy to track, and include non-technical metrics, like employee security training, along with technical metrics.

66%

of CIOs don't have cybersecurity and risk KPIs that are regularly reported to executives.

57%

of CISOs noticed that the senior management team is requesting more reports on data security than a year ago.

42%

of respondents are expecting their budget for data security to grow in 2020. For 58% of IT teams, funding will increase by 24% or less.

Diagram 13. Is your senior management requesting more reports on data security than a year ago?

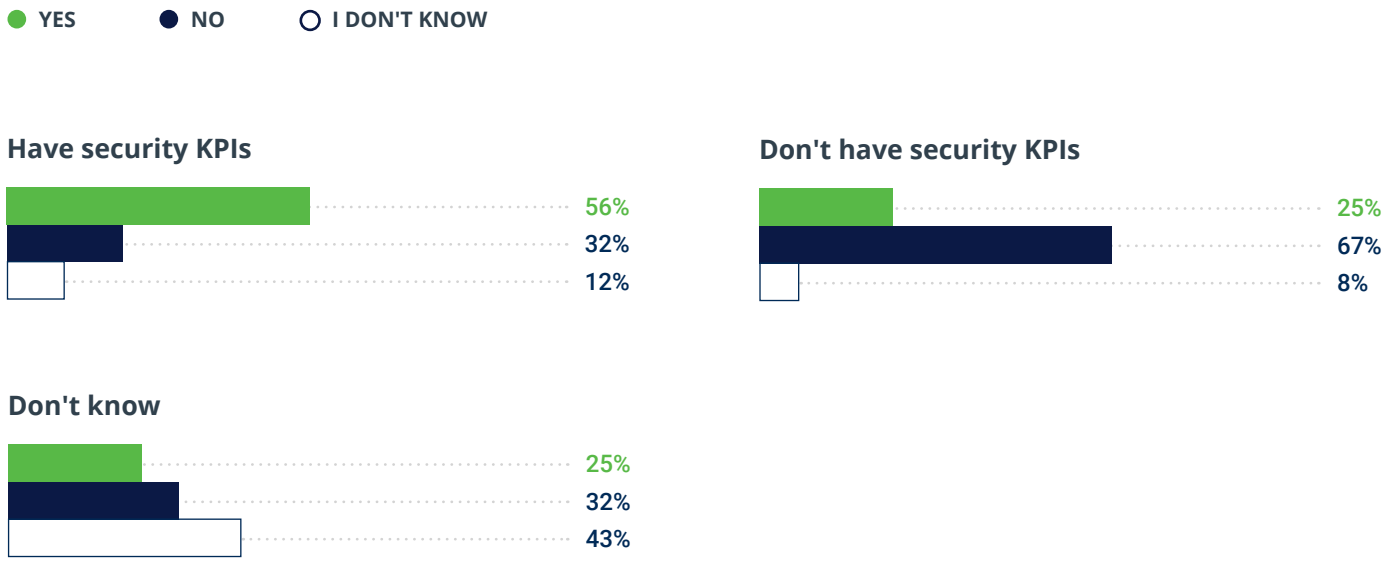
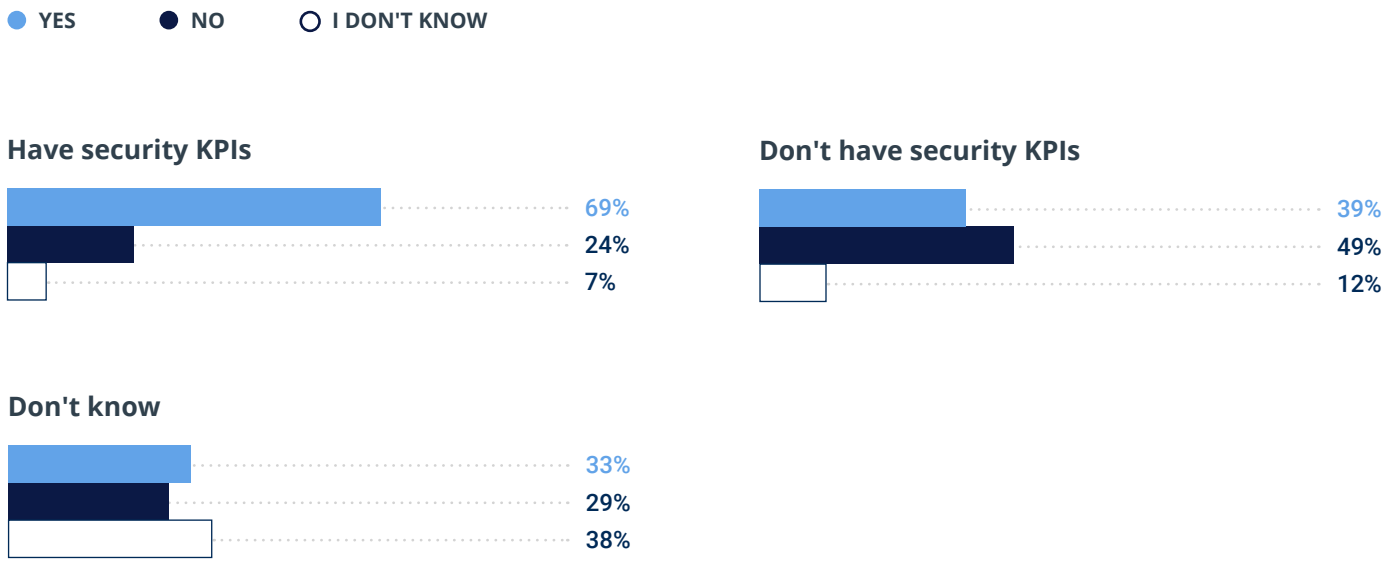


Diagram 14. Share of organizations that anticipate an increase in budget for data security in 2020



APPENDIX 1:

FINDINGS BY VERTICAL

GOVERNMENT

INCIDENTS ARE MOST COMMON DURING THE DATA USAGE STAGE.

The public sector is most prone to security mishaps during the data usage phase. 27% of agencies experienced misuse of sensitive or regulated data in the past 12 months, more than any other vertical, and one in five of them reported that the incident resulted in data compromise. Most (62%) of the organizations in this group review access rights only occasionally or not at all.

Most (75%) of public sector organizations that do not classify data upon creation required days to detect data misuse and none could do it in minutes, while those who do classify their data can spot misuse in minutes (25%) or days (38%).

DSARS ARE INCREASING.

The GDPR definitely affects the routine of IT teams in the public sector. A third of organizations saw a spike in the number of DSARs during the past 12 months, which was the highest among all verticals, and half of them reported that the cost of DSARs increased by 25%–49%. Across the sector, IT teams spend from 3 hours up to 3 days to process each request. 100% of the respondents who said that DSARs put no pressure on their IT teams have ongoing data classification and fast search through tags.

SECURITY BUDGETS ARE GROWING.

When asked about the future, 32% of respondents in the sector said that their senior management teams are requesting more reports on the state of data security than they did a year ago, and they expect this trend to continue in 2020. Also, 45% of agencies anticipated an increase in budget for data security; 55% of them expect an increase of 24% or less, while 24% expect an increase of 25%–49%. Historically, IT teams in the public sector had to push for security funding; we are pleased to see that this has changed.

25% of CIOs don't have cybersecurity and risk KPIs that are regularly reported to executives.

88% of respondents were sure that their agencies store data securely, but 24% of them discovered sensitive data outside of designated secure locations, it was left overexposed for months.

56% of government agencies don't track data sharing at all.

30% have implemented a data retention program, which is more than any other industry.

FINANCE

SECTOR EARNS TOP MARKS FOR SECURITY CONTROLS.

Perhaps because it is one of the most regulated industries, the financial sector has security controls nailed down better than other vertical. Almost half (49%) of these organizations have established continuous data discovery and classification, 54% regularly review access rights, and 81% of the ones that subject to the GDPR are confident that they don't gather more data than necessary. Hats off!

In addition, half of financial organizations can spot misuse of sensitive and regulated data in minutes, while discovery takes days, weeks or even months in other verticals. Interestingly, 79% of financial organizations that don't classify data upon creation still consider low visibility into data creation to be a security risk.

CUSTOMER DATA IS AT RISK.

The most challenging task for the financial industry is ensuring data security and privacy: 33% of respondents said they discovered sensitive or regulated data outside of designated secure locations — even though 38% of them were absolutely sure they have everything under control. Another issue is ensuring secure data access: 40% of respondents said their IT teams had granted direct access to sensitive data based solely on a user request during the past 12 months, which is the highest result across all verticals surveyed.

PRIVACY REGULATIONS WILL INCREASE IT WORKLOAD.

32% of financial organizations have already experienced an increase in DSARs, which is the highest rate among all verticals surveyed. Of those organizations, 73% report that the requests put significant or moderate pressure on IT staff, and 27% say they have increased expenses. Notably, most organizations that classify data upon creation reported a lower increase in costs associated with DSARs (1%–24%) than most organizations that don't (25%–49%).

5% of financial organizations had incidents during all 6 stages of data lifecycle.

75% of financial organizations that classify data can detect data misuse in minutes, while those who don't mostly need days (43%) or months (29%).

70% of incidents of unauthorized data sharing led to data compromise.

44% of CISOs and CIOs don't have or don't know whether they have KPIs for IT security and risk.

HEALTHCARE

SECTOR GETS WORST MARKS FOR CONTROLLING ROT.

Healthcare providers gather a substantial amount of personal data about their patients, and HIPAA requires them to retain certain types of documents (e.g., privacy policies and dispositions of complaints) for six years after creation. Still 60% of CIOs at these organizations find it difficult to identify redundant, obsolete and trivial files (ROT) that should be purged. Data classification technology can help: 43% of organizations that classify their data say they can easily identify ROT in their IT environments, as opposed to just 13% of those who don't classify their data.

Moreover, only 20% of healthcare organizations delete ROT data regularly. One reason is that 69% of healthcare providers don't have a data retention program in place to help them methodically delete information when it is no longer needed; this is the highest result across all industries surveyed.

THERE'S A WIDESPREAD BUT FALSE SENSE OF SECURITY.

More than half of healthcare organizations (52%) are certain that their regulated data is stored securely — but 24% of those reporting that absolute confidence actually discovered data outside of dedicated locations during the past 12 months.

The healthcare sector also reports more confidence in control over data sharing among employees than other industries, with 65% of respondents claiming that their employees do not share data via cloud apps to circumvent IT control. But they cannot actually verify that claim, since 32% of them don't track data sharing at all and 17% can only do it manually.

METRICS WILL BE INCREASING IMPORTANT.

47% of healthcare organizations expect their budgets to increase in 2020; 69% of them anticipate a jump of up to 24%. However, only 16% have security metrics to justify investments to senior management, so using that budget could prove difficult. Developing meaningful KPIs to prove the effectiveness of security efforts will be a key focus in 2020; 30% of organizations say that their management teams are already requesting more data security reports than they did a year ago.

55% of healthcare organizations don't regularly review access rights to sensitive data, and 70% fail to do so for archived data. Both practices violate § 164.308 of HIPAA.

88% of healthcare organizations believe that insecure data sharing poses risk to their digital transformation.

55% of healthcare organizations say that managing DSARs puts significant or moderate pressure on their IT teams. Those that classify their data, however, can satisfy DSARs in about 1/3 of the time required by organizations that don't have data classification.

EDUCATION

OVEREXPOSED DATA IS THE TOP RISK.

The highest number of incidents in the education sector happen during the data storage stage. 28% of respondents discovered data outside of secure locations, which is the highest number of all industries surveyed. Moreover, many of them admitted that this data was left exposed for days (40%) or months (33%). 47% of the organizations that discovered data outside of secure locations don't classify data at creation.

Educational organizations also suffer from weak access controls. One quarter (24%) of them admit granting access rights based solely on user requests, and another 22% said they don't know how exactly access rights are granted in their organizations — the highest percentage among all industries. To make matters worse, 63% of educational organizations don't review permissions regularly.

THE CLOUD IS BOTH AN OPPORTUNITY AND CHALLENGE.

Moving to the cloud can help organizations optimize workflows and reduce the IT complexity — but uncontrolled sharing of data in the cloud can put sensitive data at serious risk. Half of respondents (54%) in the educational sector say employees put data at risk by sharing data via cloud apps outside of IT knowledge, which is the highest percentage among all verticals surveyed. Unfortunately, 82% of educational organizations either don't track data sharing at all or do it manually, so it's not surprising that 50% of them suffered a data breach due to unauthorized data sharing during the past 12 months.

BUDGETS WILL CONTINUE TO BE TIGHT.

44% of educational organizations don't expect their cybersecurity budgets to grow in 2020, and another 31% do not know whether there will be any changes. Among those who will get additional funding for data security, the majority (62%) expect an increase of no more than 24%.

A significant issue related to budgets is lack of justification for cybersecurity investments: Only 8% of educational organizations have developed security and risk KPIs for IT leaders, and 15% are already required to provide regular reporting to management.

32% of respondents say their organizations gather and store more personal data than necessary.

ONLY 4% of educational institutions have implemented a data retention program, which is the lowest percentage among all verticals.

57% of respondents rarely or never delete ROT, which more than any other sector.

37% of educational organizations regularly review access rights to sensitive data, which is the lowest result among all verticals surveyed.

APPENDIX 2:

RESULTS BY MACRO REGION

NORTH AMERICA

DATA IS MOST AT RISK DURING STORAGE.

One in four organizations in North America detected regulated or sensitive data outside of secure locations, even though nearly all of them (90%) were sure that this data is stored securely. In fact, the highest share of incidents for these organizations occurred during the data storage stage.

The ability to classify data directly affects how well organizations can detect overexposed data. Respondents that classify data can spot it in minutes (24%) or days (45%), while those who don't classify need days (46%) or weeks (29%). As a result, data classification reduces the average time that data is exposed.

MOST ORGANIZATIONS ARE NOT READY FOR THE CCPA.

86% of CISOs and compliance officers in North American organizations subject to the CCPA are not sure whether their organizations gather and store more consumer data than necessary, even though the law obliges them to gather PII only for legitimate business purposes, and storing data you don't need puts your company at unnecessary risk.

LACK OF KPIs COULD LEAD TO PROBLEMS.

Almost half of respondents in North America (42%) say they will get more budget for data security in 2020. But 46% of them also note that their management teams are requesting more reports on the state of data security than they did a year ago, and only 26% have specific IT security and risk KPIs to submit. Without adequate metrics about the effectiveness of security solutions and other initiatives, the IT team may find their results do not meet management's expectations or that they cannot answer the question of how well the money was spent.

WHAT THE CCPA SAYS ABOUT DATA COLLECTION

1798.100 (b):

> A business that collects a consumer's personal information shall, at or before the point of collection, inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used. A business shall not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice consistent with this section.

60%

of North American organizations reported a compromise of their archived data.

29%

of CISOs at North American organizations that are subject to the CCPA don't classify data.

75%

of CDOs consider low visibility into data creation to be a compliance and security risk.

28%

of system administrators granted access to regulated data based solely on a user request.

EUROPE, THE MIDDLE EAST AND AFRICA (EMEA)

The speed of incident detection depends strongly on whether organizations classify their data at the point of creation. Organization that store PII and have classified their data can detect overexposed data in minutes (36%) or days (36%); those who have not classified their data need days (50%), weeks (33%) or even years (17%).

DATA CLASSIFICATION SLASHES THE BURDEN OF DSAR REQUESTS.

66% of EMEA organizations think that DSARs put additional pressure on IT teams. On average, they spend 36 hours to satisfy each request. However, organizations that classify their data slash that time to just 9 hours, while those who don't classify their data need 5.6 days.

SECURITY BASICS ARE OFTEN OVERLOOKED.

One in five organizations (18%) in EMEA discovered sensitive data outside of secured locations during the past year, even though 90% of them were sure that the regulated data was stored securely. In 60% of the cases, data was left overexposed for days. The majority (81%) of organization who suffered these incidents are subject to the GDPR.

Another factor that increases the risk of security incidents during data storage is the failure to properly control access rights. 73% of EMEA organizations that discovered data misuse during the past 12 months admit that they have granted access rights based solely on a user request.

COMMUNICATION BETWEEN IT AND THE C-SUITE IS LACKING.

Business leaders in EMEA organizations are the least engaged in cybersecurity issues. Only 23% of respondents say that their executive teams request more reports on the state of data security than they did a year ago, which is the lowest among all regions analyzed. Just 37% of IT teams expect a budget increase in 2020, which is also the lowest number globally.

Only 16% of respondents have cybersecurity KPIs that are regularly reported to executive management, even though the GDPR requires tracking metrics such as the volume of DSAR requests and the rate of on-time completion.

58%

of EMEA respondents are unsure whether their organization collects more customer data than necessary.

56%

of CIOs and 88% of CISOs consider low visibility into data being created to be a compliance risk.

ONLY 8%

of organizations say they can spot unauthorized data sharing incident in minutes; 62% say detection takes days, and 23% say it take weeks.

Every third

incident of data misuse resulted in a data breach.

58%

of EMEA respondents are unsure whether their organization collects more customer data than necessary.

56%

of CIOs and 88% of CISOs consider low visibility into data being created to be a compliance risk.

ASIA-PACIFIC (APAC)

THE REGION HAS THE LEAST CONTROL OVER DATA SHARING.

22% of APAC organizations report a data sharing incident during the past 12 months, which is the highest rate among all regions analyzed. In 56% of the cases, it took days to discover the incident, and half of the incidents resulted in a data breach.

The rate of cloud adoption across the APAC region is high, and many organizations now store and share sensitive and regulated data in the cloud. However, the majority of APAC organizations lack automated tools to monitor user behavior. Since 26% track data sharing manually and 28% do not track it at all, it's no surprise that half of organizations who had data sharing incidents believe that their employees share data via cloud applications outside of IT control.

IDENTIFYING AND DISPOSING OF ROT DATA IS A KEY CHALLENGE.

Many APAC respondents are subject to compliance regulations such as the GDPR (38%), HIPAA/HITECH (23%) and PCI DSS (21%). The GDPR requires organizations to delete EU citizen data as soon as it is no longer needed. However, only 28% of APAC organizations have a data retention program to get rid of irrelevant records in a timely manner; indeed 63% of CISOs and 67% of CIOs admitted that they find it difficult to even identify ROT data in their IT systems. Therefore, it's not surprising that 35% of APAC organizations delete ROT only occasionally, and another 30% rarely or never delete it.

89%

of APAC organizations are sure that regulated data is stored in a secured location, but 19% have discovered sensitive data outside of designated locations in the past 12 months.

71%

of data misuse incidents led to data compromise.

58%

of APAC organizations occasionally or rarely review access rights to sensitive data.

100%

of those who had unauthorized data sharing incidents believe that insecure data sharing poses risks to digital transformation.

ONLY 21%

of respondents have IT security and risk KPIs that are regularly reported to executive management or the board of directors.

APPENDIX 3:

RESULTS BY MICRO REGION

UNITED STATES

DATA DISPOSAL IS LACKING, DESPITE THE REACH OF THE GDPR.

We were surprised to find out that 77% of U.S. organizations don't have a data retention program. Of those, 79% don't get rid of ROT files regularly (they do it either occasionally or never), and 63% find it hard to identify unnecessary data. Moreover, the majority of U.S. organizations that have a data retention program are subject to the GDPR, which requires organizations to remove customer data at the end of its data lifecycle.

LOW VISIBILITY INTO DATA WILL RESULT IN CCPA COMPLIANCE ISSUES.

69% of organizations subject to the CCPA are unsure whether they store more customer data than necessary, even though this standard obliges organizations to store only the data necessary for achieving business objectives. This problem primarily affects organizations that don't classify their data, which is about half of all U.S. companies: Only 10% of those who do not classify their data are sure that they don't store more customer data than necessary, as compared to 96% of those who continuously classify data. Lack of data classification, along with the failure to remove ROT data, will hinder them from efficiently managing DSARs.

67% of CIOs in the United States don't have IT security and risk KPIs.

30% of U.S. respondents reported that employees share data via cloud applications outside of IT control.

Half of incidents of unauthorized data sharing led to data compromise.

86% of respondents believe that insecure data sharing poses risks to digital transformation, though 63% of them either don't track data sharing or do it manually.

Every fourth organization found regulated data outside of secure location, even though 88% of them were sure that they store this data only in safe places.

UNITED KINGDOM

CONFIDENCE ABOUT DATA SECURITY IS MISPLACED.

27% of UK organizations have discovered sensitive data outside of dedicated locations in the past year, even though 91% of them were sure that sensitive data is stored securely. Data was left overexposed for days (33%) or weeks (22%). The majority of this group (63%) failed to classify their data at the point of creation. 90% of those who had data overexposure are subject to the GDPR.

45% of UK respondents that must comply with the GDPR are unsure whether their organizations gather more customer data than necessary.

10% of organizations have experienced a misuse of sensitive data in the past 12 months. In every third case, data was compromised.

15% of organizations have mistakenly deleted necessary, sensitive or regulated data over the past year.

UNAUTHORIZED DATA SHARING IS WIDESPREAD.

14% of UK respondents experienced security incidents due to unauthorized data sharing, and half of those incidents resulted in data compromise. In addition, 39% of UK respondents are sure employees in their organizations share sensitive data via cloud applications outside of IT control. Indeed, UK organizations can hardly control user activity, since nearly a third of them (29%) do not track data sharing at all and 18% do it manually.

82% of UK organizations believe that insecure data sharing poses risks to digital transformation.

59% think it is difficult to get rid of ROT data.

DSARs PUTS ADDITIONAL PRESSURE

According to a report from the Information Commissioner's Office (ICO) about the first year of the GDPR, DSARs are the most frequent type of data protection complaint from the public (38%). It is challenging for organizations to respond DSARs within 30 days, especially when they receive thousands of them. In fact, 72% of UK respondents said that the need to deal with DSAR requests puts additional pressure on their IT teams. But organizations that have their data classified and can easily search through it say they can respond to a DSAR in 5 hours, while those who don't spend three times longer.

46% don't have security KPIs that are regularly reported to management.

FRANCE

VISIBILITY INTO DATA SHARING IS POOR.

The most problematic stage for French organizations is data sharing: 22% of respondents experienced a security incident due to unauthorized data sharing in the past 12 months. One third (33%) of them think employees in their organization share data via cloud applications outside of IT control or knowledge. Of those, none of French organization has automated processes to track data sharing among employees. Investing in automated solutions for user activity monitoring can minimize the risk of insecure data sharing.

FAILURE TO DELETE DATA IS A WIDESPREAD PROBLEM.

We were surprised to find out that 88% of French organizations have not implemented any data retention program, which is the highest percentage of all the countries analyzed. A similar number (87%) struggle to identify ROT data. Moreover, 13% have deleted sensitive or regulated data by mistake during the past year; all of them lack both data classification and a data retention program. What is more worrying, all of them store PII and need to comply with the GDPR.

MANY ARE IN VIOLATION OF THE GDPR.

77% of French organizations that are subject to the GDPR are unsure whether they store more customer data than necessary. Of those, 44% do not classify data at the point of creation. Since a fundamental requirement of the GDPR is to collect only business-critical data from EU citizens, many French organizations are at high risk of steep fines for non-compliance.

73% of French organizations consider low visibility into data creation to be a security and compliance risk.

100% of French organizations believe that insecure data sharing poses risks to digital transformation.

11% experienced misuse of sensitive or regulated data in the past 12 months.

50% of respondents rarely get rid of ROT, and 38% do it only occasionally.

8% of French organizations have been fined for non-compliance in the past 12 months.

GERMANY

LACK OF PROPER DATA DELETION WILL INCREASE GDPR RISKS.

78% of German organizations have not implemented any data retention program, even though 92% of respondents must comply with the GDPR, which requires them to delete customer data that they no longer need. Organizations that attempt to correctly dispose data often fail: Every fifth (22%) German organization has deleted sensitive data by mistake in the past 12 months.

In addition, the vast majority of German respondents (89%) struggle to identify ROT data. However, once again, data classification makes a difference. German organizations that do not classify their data get rid of ROT rarely (67%) or occasionally (33%); however, 20% of those who do classify their data purge ROT regularly, while 40% do so occasionally and 40% do it rarely.

DATA OVEREXPOSURE IS CORRELATED WITH FAILURE TO FOLLOW DATA SECURITY BEST PRACTICES.

10% of German organizations have discovered sensitive or regulated data outside of designated secure locations over the past year, even though 90% of them were sure that regulated data was stored securely. Data was generally left overexposed for days. Of those, half of organizations admit they granted access rights based solely on a user request during the past 12 months.

DATA CLASSIFICATION SLASHES DSAR PROCESSING TIME.

Almost half (44%) of German organizations reported an increase of up to 24% in costs associated with DSARs. Nearly all (99%) of respondents say the need to deal with DSAR requests puts additional pressure on IT teams, which is the highest number compared to other countries analyzed. Organizations that classify their data need 2 hours to process one DSAR while those who do not classify spend 5 hours.

73% of German organizations are unsure whether their organization gathers and stores more customer data than necessary.

100% believe insecure data sharing poses risks to digital transformation.

44% do not track data sharing among employees.

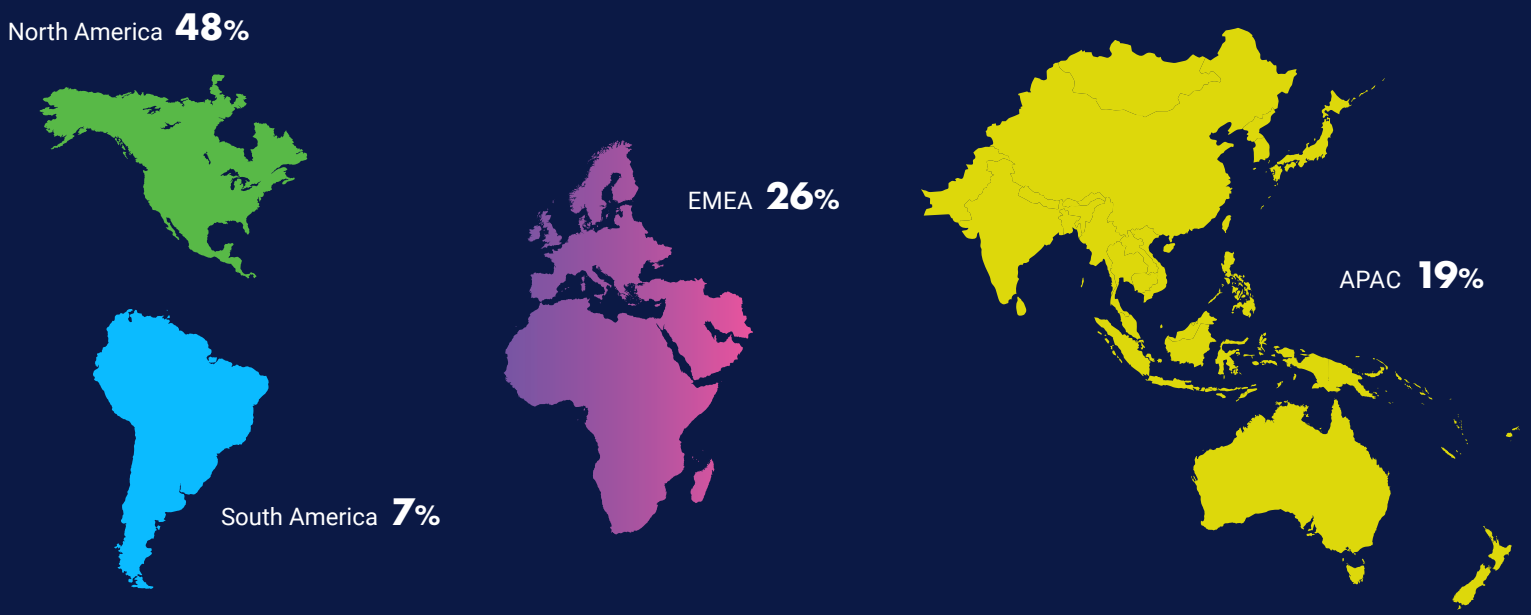
56% do not have data security KPIs that are regularly reported to management.

55% anticipate a budget increase for data security.

APPENDIX 4:

SURVEY DEMOGRAPHICS

ORGANIZATION LOCATION

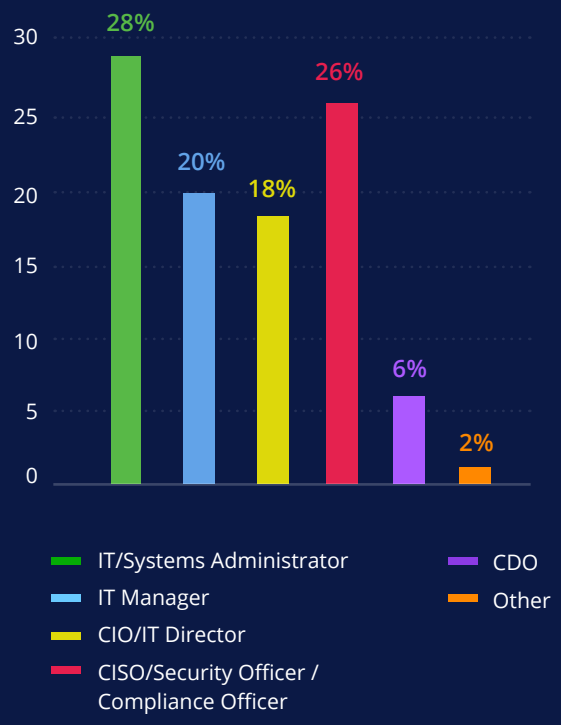


ORGANIZATION SIZE

TOP INDUSTRIES REPRESENTED

Health Care	10%
Finance	9%
Government	9%
Manufacturing	8%
Technology/Software	8%
Education	7%
Service	4%
Consulting	4%
Non-profit	4%
Retail & Wholesale	3%

TOP JOB TITLES REPRESENTED



ABOUT THE REPORT

The report is brought to you by Netwrix Research Lab, which conducts industry surveys among IT pros worldwide to discover up-to-date interests and granular trends' analysis of the industry. For more reports, please visit: www.netwrix.com/go/research

ABOUT NETWRIX

Netwrix is a software company that enables information security and governance professionals to reclaim control over sensitive, regulated and business-critical data, regardless of where it resides. Over 10,000 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:
300 Spectrum Center Drive, Suite 200, Irvine, CA 92618
Phone: 1-949-407-5125 **Toll-free:** 888-638-9749 **EMEA:** +44 (0) 203-588-3023

www.netwrix.com/social

Copyright © Netwrix Corporation. All rights reserved. Netwrix is trademark of Netwrix Corporation and/or one or more of its subsidiaries and may be registered in the U.S. Patent and Trademark Office and in other countries. All other trademarks and registered trademarks are the property of their respective owners.