Annual Data Exposure Report 2023

code42

Forward: A Note from Code42 President & CEO

Five years ago we launched our first Data Exposure Report (DER) with the goal of examining the problem of data loss from insiders. The terminology evolved over time as we analyzed insider threats — and then Insider Risk. Whatever you call it, it was not a new problem — but one that continued to become more urgent and complex due to a number of key drivers. Over the past five years, the research continually revealed that our complex digital landscape, mixed with the realities of human behavior, was creating challenges for businesses across industries.

> **In the past, DER has focused on uncovering the key drivers of Insider Risk: digital transformation, workforce turnover, hybrid-remote work and the continued adoption of cloud technologies. This year, our goal was to understand the specific challenges related to building and maintaining Insider Risk programs, technologies and training. It's clear that awareness of Insider Risk is growing, yet many companies still struggle with setting up effective programs.**

At Code42, we believe that protecting data and reducing Insider Risk should not come at the expense of fostering an open and collaborative culture. In order to be competitive, companies need to accelerate growth, foster innovation and drive productivity — managing Insider Risk should not stand in the way of that.

Joe Payne

President & CEO
Code42

TL;DR — Key Findings

Insider Risk is emerging as one of the most difficult threats to detect in today's environments. Business and security leaders are increasing their focus on this growing problem. Security teams are demanding improvements in technology, training and programs, as detecting and responding to data exfiltration from insiders is challenging to solve. This is driving an urgent need to overcome the challenges associated with managing Insider Risk – an issue that is becoming increasingly complex to solve. This year's DER uncovered the following data.

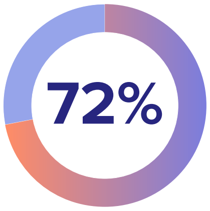
Data loss from insiders is a growing problem despite 72% of organizations having a program dedicated to Insider Risk

32%

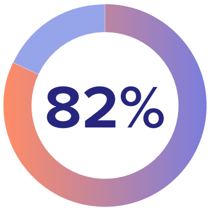
The average year-over-year increase in the estimated monthly number of insider-driven data exposure, loss, leak and theft events

$16M

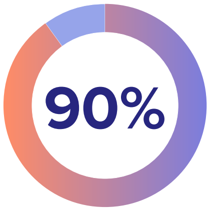
Insider-driven data exposure, loss, leak and theft events could cost companies $16 million per incident, on average.



Despite 72% of companies having a dedicated program to Insider Risks/threats, 71% expect data loss from insider events to increase at their company in the next 12 months.



Over four in five CISOs admit data loss from insiders is a problem for their company.



Companies are leveraging multiple technologies to protect and manage Insider Risk — with the majority (90%) using a combination of IRM, DLP, CASB and UEBA to protect data from exfiltration by insiders.

Cybersecurity teams recognize that **detecting, responding to and mitigating data exfiltration events** from insiders is challenging and that Insider Risk is one of the hardest cybersecurity threats to detect

CISOs rank the **most difficult type of threats** to detect

#1 Insider Risk
#2 Cloud data exposure
#3 Malware/ Ransomware

The move to **hybrid work** is increasing the need for **data security training** but most companies are still struggling to deliver high-quality methods

81%

Over four out of five believe the new hybrid-remote workforce has increased the need for data security training in their company.

96%

But nearly all feel their data security training requires improvement.

Objective of the Annual Data Exposure Report: 2023

In past Annual Data Exposure Reports, Code42 has researched the key drivers of Insider Risk. In the 2023 edition, we wanted to understand the specific challenges related to building and maintaining Insider Risk programs, technologies and training.

To explore this, we surveyed 700 respondents – cybersecurity leaders, cybersecurity managers and cybersecurity practitioners – from US companies with 500 or more employees from a range of public and private sectors. Full demographics of surveyed individuals can be found on page 18.

Part 1

Introduction

The headlines in 2022 were dominated by cases of IP theft and insider threats. Pharmaceutical company Pfizer **sued two former employees**, accusing them of stealing “the hard work” of the company’s scientists, including trade secrets related to diabetes drug research, and taking that information to start their own competing drug company. Two Johnson & Johnson subsidiaries **accused three former employees** of “the shameless, systematic and ongoing misappropriation of trade secrets.” They alleged that the ex-workers went on to share the stolen documents — which included source code, product designs and details of test cases — with Noah Medical, their current employer, another maker of robotic surgery systems. And, in probably the biggest Insider Risk case we’ve seen in years, coding automation company Appian **was awarded $2 billion in damages** for trade secret misappropriation after a jury found that low-code platform provider Pegasystems hired an employee of a government contractor to essentially spy on Appian to learn how to better compete against its rival.

It’s been over a year since we published our **2022 Data Exposure Report**, and the magnitude of data loss from insiders (aka Insider Risk) is staggering. It remains an increasingly pervasive problem to solve — with a year-over-year increase of 32% in the number of Insider Risk incidents. The workforce is changing faster than ever as we’ve entered a new era of work. Cybersecurity teams are struggling to keep up with and manage Insider Risk, which is driving the urgent need to address it.

From the rush to remote work in 2020 to the new **hybrid-remote world**, the way employees work and collaborate has changed

Insider Risk occurs when sensitive corporate data — IP, digital assets, trade secrets, crown jewels — moves to untrusted places like personal devices, email or cloud destinations due to the behaviors of insiders, malicious or accidental. Such data movement presents considerable competitive, financial, privacy and compliance risk to the organization.

Several key factors are driving the increase of Insider Risk. Today's security teams are facing a constantly changing landscape. From the rush to remote work in 2020 to the new hybrid-remote world, the way employees work and collaborate has changed. On top of this, economic uncertainty has led to workforce volatility. A lack of confidence in job security means that many employees are taking action to protect themselves — gaining the competitive edge by downloading IP, customers' lists or sales strategy. All of this makes data protection more challenging. The continued adoption of cloud technologies compounds this.

> **Whether insider threats are intentional or unintentional, they are often more dangerous than external threats because insiders are authorized to access much of the company's data to get their job done. It remains one of the hardest cybersecurity threats to detect.**

Recent government regulations underscore the significance of the threat of data loss from insiders. The **Security and Exchange Commission (SEC) has proposed** a new set of cybersecurity disclosure rules for public companies which would require them to report "material cybersecurity incidents" to the SEC within 4 days, which will be difficult for many companies that still struggle with detection. Under the rules, companies and their senior leadership would also be required to prove their board's oversight of cybersecurity risk in the event of a material incident. This adds both operational and reputational concerns to the disclosure process.

A lack of confidence in job security means that many **employees are taking action** to protect themselves — gaining the competitive edge by downloading IP, customers' lists or sales strategy. All of this makes data protection more challenging

Separately, the **Federal Trade Commission (FTC) has proposed a new rule** to ban noncompete clauses, freeing up employees to leave for competitors. With the **total theft of U.S. trade secrets** accounting for up to $540 billion each year, there are far-reaching competitive and financial consequences if IP moves to a competitor with an employee. The proposed FTC ruling to ban noncompetes is a reminder that companies should never rely on a piece of paper to enforce what data protection protocols should do instead.

And while nearly three out of four companies (72%) say they have a program dedicated to Insider Risk or threats, conflicting data shows that these same companies are still struggling with the problem.

> **So what's the disconnect? In this year's report, we take a closer look at the challenges of implementing an IRM program. We examine how technology, budget, people and processes all influence the success or failure of an IRM program.**

72%

of companies say they have a program dedicated to Insider Risk or threats, but conflicting data shows that these same companies are still **struggling with the problem**

Part 2

Data Exposure is Getting Worse and is Expected to Grow

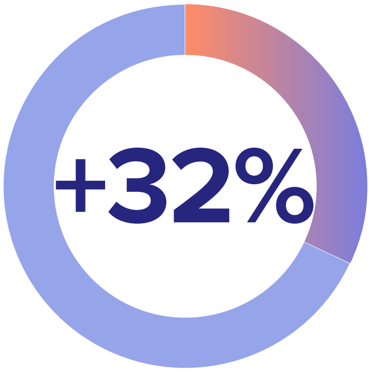
The number of data exposure events has increased by 32% year-over-year

While loose lips sink ships, loose data will capsize a company quickly. The cost repercussions of an insider-driven data exposure, loss, leak and theft event are immense, with respondents estimating it would cost their company $16 million per event, on average. That estimation is even higher for companies that cite experiencing more than 50 insider events per month — they say the cost could reach $20 million. Their direct experience with these types of events likely contributes to their estimation skewing higher. In addition to these direct costs, data loss has the potential for significant financial, reputational and operational ramifications — nevermind a company's intellectual property (IP) ending up in the hands of a competitor.

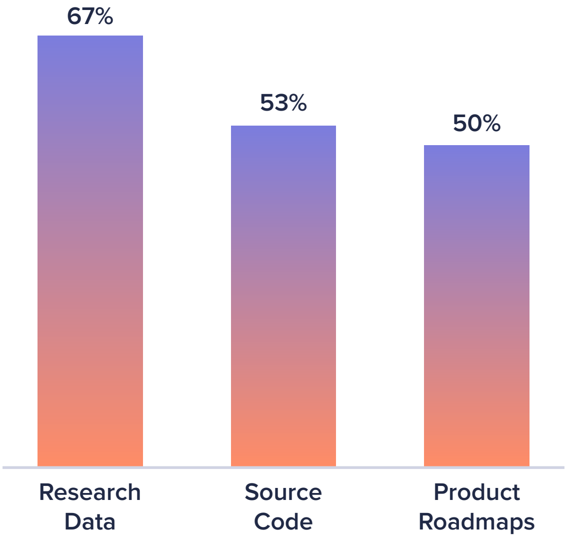
The higher the value, the greater need for protection, particularly when the data is sensitive in nature. When asked what they consider the most valuable data types, respondents ranked research data (67%), source code (53%) and product roadmaps (50%) as the three most valuable. Value was defined as the potential business loss associated with exfiltration, making it crucial that these data types are protected from internal risk.

The **2022 Data Exposure Report** highlighted the need for a better approach to protect data from Insider Risk. Unfortunately, the past year has shown no sign of improvement. Three quarters (75%) admit that data loss from

Average YoY increase in the number of insider-driven events

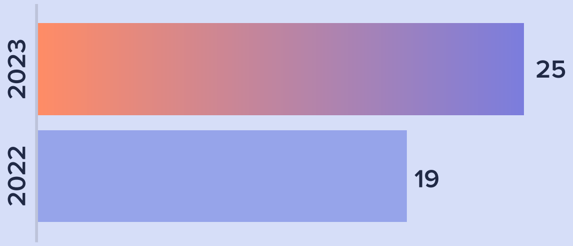


Valuable Data Types



Rank the top three data types by value/importance to your company, with value being defined by the potential business loss associated with exfiltration [700]

Number of insider-driven events per month



How many insider-driven data exposure, loss, leak and theft events do you estimate your company experiences in a month? [700]

88%

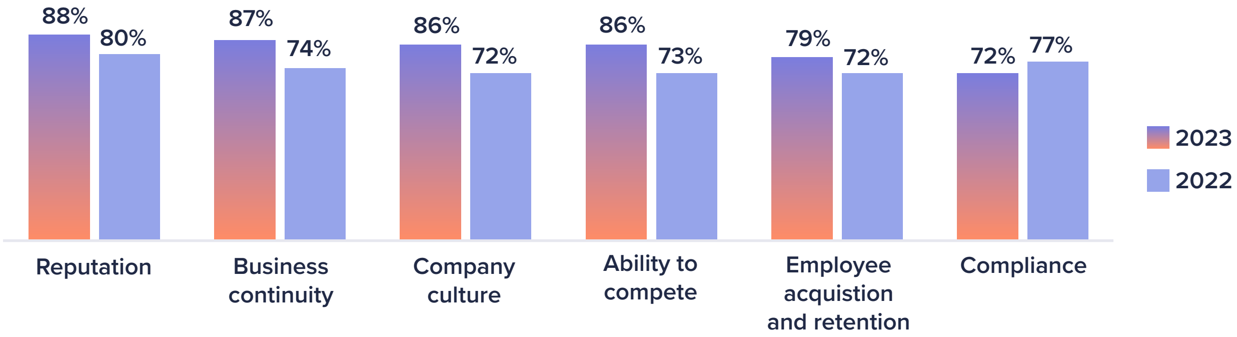
Percentage of respondents who say there would be a major or moderate impact to revenue

insiders is a problem within their company, up only slightly from our last report (73%), showing the issue has persisted.

In fact, the research suggests the issue has only worsened – since our last report there has been a 32% average increase in the number of insider-driven data exposure, loss, leak and theft events companies estimate they experience a month. This equates to an average of 300 events per company per year, increasing the likelihood of data leakage and breaches.

More companies are beginning to understand the impact that an insider event would have. Respondents say there would be a major or moderate impact to revenue (88%) and reputation (88%) following an Insider Risk event. It's not surprising that reputation is ranked so high, given the potential loss in customer, investor or partner trust following an insider event.

Major or moderate impact of an Insider Risk event involving loss or theft of sensitive information



To what extent has/would the following be impacted as a result of an Insider Risk event involving loss or theft of sensitive information in your company? [700]
Showing 'Major impact' or 'Moderate impact' combined, split by survey year

In addition, the number of respondents indicating that an insider event would impact company culture and employee acquisition/retention has increased since our last report. Insider Risk is not just a cybersecurity issue, it is intimately intertwined with a company's culture and has a significant impact on the business. Creating a culture built on trust and transparency is essential for companies in today's hybrid-remote world. Making expectations clear and defining what is expected of employees benefits all sides.

Insider Risk events range from **malicious, to negligent, to accidental** in nature. While the number of insider events has increased year-over-year, concern over the types of events has shifted slightly since our last report. When asked which of the three types of events they are most concerned about, respondents rank accidental as number one, followed by malicious and negligent. The number of respondents most concerned with accidental events increased, while those most concerned about negligent events decreased. The shift in focus from negligent to accidental could be due to two reasons:

> 1. **Lack of training/education on how to behave in a safe and secure way (more in part 5)**
> 2. **The technologies and programs in place are failing to detect and prevent accidental actions from having damaging consequences (more in part 4)**

Given the huge impact such events have, it's unsurprising that 79% of CISOs feel they could lose their job from an unaddressed insider breach.

But there are no signs of the problem getting better, with 76% of CISOs expecting data loss from insider events to increase in the next 12 months. This suggests an urgent need for companies to revisit the approaches they currently have in place.

76%

of CISOs expect **data loss from insider events to increase** in the next 12 months

A single insider-driven data exposure, loss, leak and theft event could cost companies **$16 million**, on average

79%

of CISOs feel they could lose their job from an **unaddressed insider breach**

Part 3

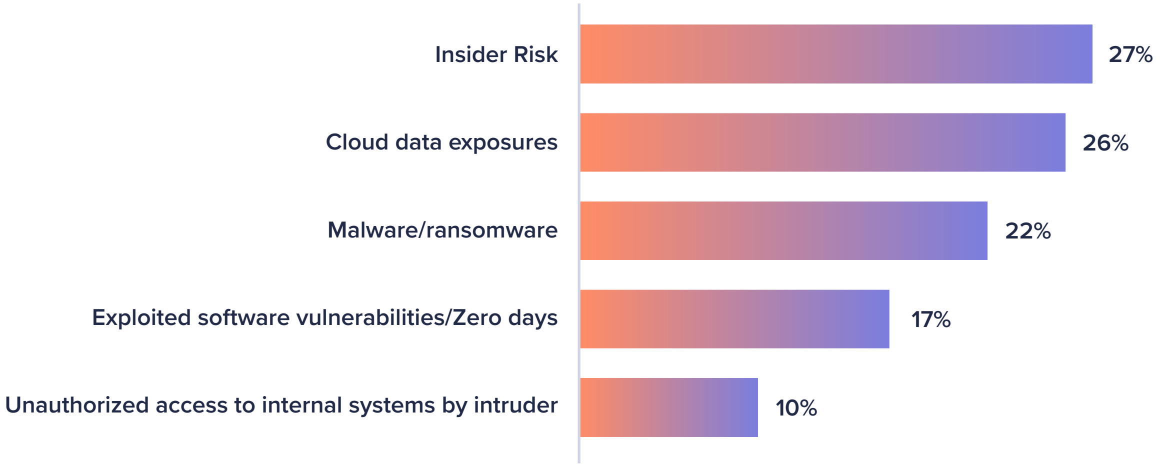
Why Is It So Hard? The Complex Challenge of Data Loss from Insiders

Insider Risk is one of the hardest cybersecurity threats to detect

Stopping data loss from insiders is a complex problem to solve. CISOs recognize this, with three quarters (75%) finding data loss from insiders difficult to detect in their company.

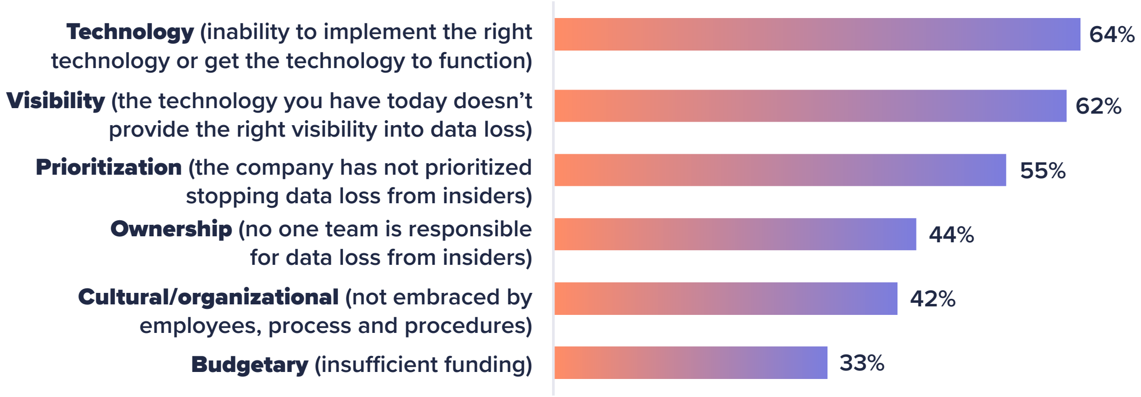
When asked what type of threat is the **most** difficult to detect in their company, CISOs ranked Insider Risk (27%) as the most difficult, placing it above cloud data exposures (26%) and malware/ransomware (22%). This may seem surprising, given the way malware and ransomware dominate today's headlines, but the data demonstrates the growing awareness around the complexity of the Insider Risk problem. Insider events are often harder to identify and remediate than those originating externally because insiders require an elevated level of trust and access to get their jobs done. This makes it critical to have an Insider Risk Management program in place.

The most difficult type of threat to detect



What is the most difficult type of threat to detect in your company's environment? [200] Showing CISO responses only

Top 3 challenges when building a program to protect against data loss from insiders

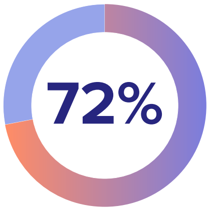


Please rank the top three challenges when it comes to building a program to protect against data loss from insiders within your company. Combination of responses ranked first, second and third [700]

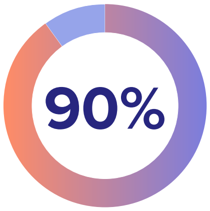
Unfortunately, while nearly three-fourths of companies (72%) have a program (budget/people/resources) dedicated to Insider Risk or threats, the data suggests that these programs are not always effective. Respondents with a dedicated program are more likely to report that Insider Risk is the most difficult type of threat to detect (25%) and that data loss from insiders is a problem for their company (77%), compared to those that don't have a program (16% and 67% respectively). This suggests the programs in place are immature and ineffective.

Building a program to protect against data loss from insiders is complex – it means mobilizing the company to address Insider Risk, from the IT and security teams to each employee. Having the right technology in place (64%) and having technology that can provide the right visibility into data loss (62%) are the top two issues faced when building such a program. Implementing effective technology that functions as intended makes the process of addressing risk much easier and more accurate – something many seem to be lacking.

With technology listed as a number one challenge to programs, one might wonder if there is a primary culprit. The answer is: organizations have too much technology and none of it works well enough for them. The majority (90%) of companies indicated they used a combination of IRM, DLP, CASB and UEBA to protect data from exfiltration by insiders. This technology overload could cause programs to be disjointed and ineffective at managing Insider Risk.



Nearly three-fourths of companies have an Insider Risk program, but these programs don't always work



of companies indicated they used a combination of IRM, DLP, CASB and UEBA to protect data from exfiltration by insiders

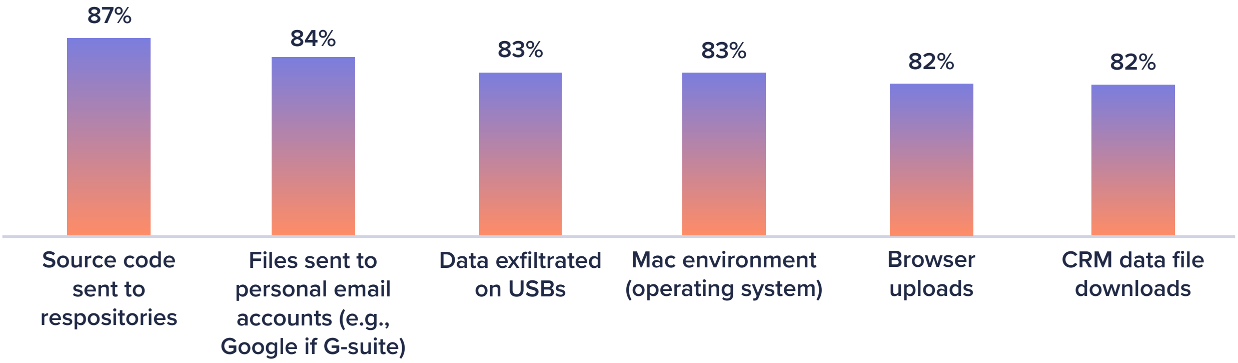
85% of companies are facing **technology/ visibility challenges** when it comes to protecting data from **exfiltration by insiders**

Compounding the challenges around Insider Risk, a shift in mindset is still needed across departments due to gaps in prioritization. Around four out of five (79%) CISOs do not feel the leadership team (board, C-suite) places enough attention on data loss from insiders. While security leaders and practitioners are becoming increasingly aware of the impact of data loss from insiders — and the urgent need to protect against it — it's clear there's still work to be done educating leadership and elevating Insider Risk to a boardroom topic, particularly given the impact potential events could have on revenue and reputation damage.

> **Similarly, we see the same proportion (79%) of CISOs reporting that their governance, risk and compliance teams fail to pay sufficient attention to data loss from insiders. Cybersecurity teams need support – from both a budgetary and compliance viewpoint — to tackle insider threats. Only 19% of companies' global cybersecurity budget is dedicated to detecting, investigating, responding and mitigating Insider Risk, on average. 69% say the budget for Insider Risk Management will increase over the next year, suggesting current budgets are insufficient.**

Most companies are facing challenges when it comes to their data exfiltration technology and recognize that greater visibility is needed. In particular, more visibility is needed into the source code sent to repositories. For many companies, source code can be the single most valuable IP to which insiders present the biggest risk, suggesting that better **source code exfiltration detection** is needed. Having technology that provides data-centric protection and visibility into the behavior of insiders is key.

More visibility is needed to protect against data exfiltration from insiders



What level of visibility does your company need over the following to protect against data exfiltration from insiders? [700] Showing 'A lot more visibility' and 'A little more visibility' combined

Part 4

Behind the Tech: How People and Processes Are Integral to an IRM Program

The need for data security training has increased, so getting it right is essential

While implementing effective technology is essential to managing Insider Risk, people are an equally important piece of the puzzle. Cultivating the right culture is essential. Nearly three-fourths of CISOs (71%) admit that monitoring their peers makes them uncomfortable. But it's possible to overcome that discomfort if a culture is built on the foundation of empathy and transparency. When employees are brought into the process in an effective way, they are empowered to make safer and smarter decisions. The best way to build this culture is through just-in-time, personalized and empathetic training and education.

However, the data shows that simply increasing the frequency of training is not enough. Those conducting weekly training are more likely to say a complete overhaul is needed than those conducting it monthly (22% vs. 10% respectively). There is also a correlation between the monthly number of insider-driven events companies experience, with those conducting training weekly suffering an average of 21% more events than those conducting it monthly.

The vast majority (93%) of CISOs say that the new hybrid-remote workforce has increased the need for data security training in their company. Additionally, nearly all companies (96%) feel that improvements are needed in training with two-thirds (66%) stating that a complete overhaul

71% of CISOs admit feeling uncomfortable **monitoring their peers**

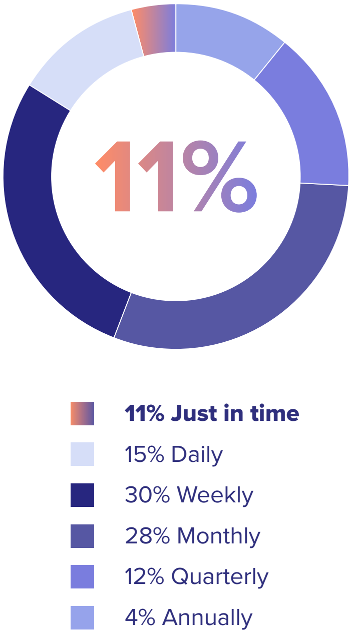
93% of CISOs say the **hybrid-remote workforce** has increased the need for **data security training**

is needed. 58% of companies conduct training on a routine schedule (weekly or monthly), while the remainder only conduct training when there are increased risks, such as a new employee starting or a cyber-risk event occurring. Over time, the frequency of routine training has increased, with 58% doing so weekly or monthly. Only 11% of organizations conduct just-in-time training — and this may be why so many companies say a complete overhaul is needed. Gartner® Innovation Insight on Security Behavior and Culture Program Capabilities, published November 2022 states that "84% of cybersecurity leaders want to mitigate risk by managing employee behavior, yet under half (43%) consistently track behavior and few deploy effective solutions." Gartner recommends looking at Security behavior and culture program (SBCP) solutions that embrace both technical and nontechnical emerging capabilities, including personalization, automation, behavioral science, data integration and omnichannel engagement.

This supports that training needs to be at the right time — when the employee is taking an action that is putting company data at risk — in a personalized and integrated way. This builds a culture of security and extends the burden of risk reduction beyond the security team to truly 'democratizing' it to all employees.

Over the past few years, the rules of engagement have been rewritten as digital transformation initiatives accelerated. If you do not have the right training and education in place, it's likely that employees' ingenuity will make up for the gaps by finding creative (and usually unsanctioned) ways to collaborate with their dispersed colleagues.

Frequency of Data Security Training



How often is employee data security training conducted at your company? [700]

Part 5

Conclusion

Insider Risk remains one of the hardest cybersecurity threats to detect, and the results make it clear that data loss from insiders is a growing problem. It is also a complex problem to solve because insiders must rightfully handle and share data every day to get their jobs done, and this requires access to valuable data and systems. Threats manifest as malicious, accidental and negligent, making detection and response even more challenging. This year's Data Exposure Report is a real call-to-action for the security industry to do better. With 90% of organizations using a combination of 4-5 technologies, we must make the lives of security professionals easier by building a more complete and holistic solution that detects, prioritizes, responds to insider threat events and helps reduce overall Insider Risk in the organization. In the meantime, there are several things security professionals can do to build more resilience against insider Risks:

1 **Ensure the technology used is easy to administer and provides robust visibility over *all* data**, including unstructured data, research data and source code. Prioritizing speed of implementation and ease of use might just be the key between the success or failure of a program.

2 **Strengthen program efforts by building a culture on the foundation of transparency**, where employees understand expectations and are held accountable for their actions. Train the security team to take an empathetic approach when dealing with their employees and implement just-in-time training to correct user behavior in real time.

Part 6

Methodology

Code42 commissioned independent market research agency Vanson Bourne to conduct the Data Exposure Research. The 2023 study surveyed 700 respondents (300 cybersecurity practitioners, 200 cybersecurity managers and 200 cybersecurity leaders) from companies headquartered in the US in January and February 2023. These companies had 500 or more employees and were from a range of sectors, including automotive and aerospace/manufacturing, business and professional services, energy, oil/gas and utilities, technology, pharmaceutical and life sciences/biotechnology, among other sectors.

Vanson Bourne conducted the 2023 and **2022** Annual Data Exposure Reports. Code42 has in the past worked with other research firms and previously published Annual Data Exposure Reports in **2018**, **2019**, **2020** and **2021 Volume I** and **2021 Volume II**.

All interviews were conducted using a rigorous multi-level screening process to ensure that only suitable candidates were given the opportunity to participate.

This report sometimes references data from the **2022** Annual Data Exposure Report. Please note there have been slight wording changes between the surveys, of which full details can be provided if required. Where there are wording differences, we have used the 2023 wording. In addition, the scope has had some changes so caution has been taken when making comparisons to 2022 iterations. The main differences include:

- Respondent type: the 2022 report consisted of business decision makers, cybersecurity leaders/managers and cybersecurity practitioners
- Sector: the 2022 report consisted of a slightly different sector list

About Gartner

GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

About Code42

Code42 is the leader in Insider Risk Management, offering complete data loss detection and response solutions. Code42 Incydr™ is native to the cloud and rapidly detects and prioritizes data exposure events and offers a complete range of response solutions. These include automated micro-learning modules for accidental non-malicious risk, case management for rapid and easy collaboration on investigations, and automated blocking for the highest risk use cases. Code42's full suite of expert services help get an organization up and running and mature its processes and reporting. With Code42, security professionals can protect corporate data and reduce Insider Risk without putting extra burden on security teams or slowing down legitimate collaboration of employees. Designed to meet regulatory control requirements, Code42's IRM solution is FEDRAMP authorized and can be configured for GDPR, HIPAA, PCI and other compliance frameworks. Innovative organizations, including the fastest-growing security companies, rely on Code42 to safeguard their ideas. Founded in 2001, the company is headquartered in Minneapolis, Minnesota, and backed by Accel Partners, JMI Equity, NewView and Split Rock Partners. Code42 has played a defining role in developing a vision and requirements for the IRM category and is a founding member of the annual Insider Risk Summit and Insider Risk Community.

The Company has several offices across the United States and its clients include large multinational organizations, such as CrowdStrike, Exabeam, BAYADA Home Health Care, Lending Club, MacDonald-Miller, MACOM, North Highland, Ping Identity, Shape Technologies, Snowflake, University of Georgia, User Testing, UTEX and Xactly.

About Vanson Bourne

Vanson Bourne is an independent specialist in market research for the technology sector. Their reputation for robust and credible research-based analysis is founded upon rigorous research principles and their ability to seek the opinions of senior decision makers across technical and business functions, in all business sectors and all major markets.

For more information, visit **www.vansonbourne.com**.