mimecast

Annual Data Exposure Report 2024

mimecast

Foreword

Code42, now a Mimecast company, undertakes substantive undertakes substantive research on the risks and threats created by insiders (employees and contractors). We talk to over 700 security professionals to ensure the findings have statistical significance and that we can rely on the data. We share this research broadly at no cost as one of the ways we give back to the security community. This year's annual Data Exposure Report (DER), has some interesting findings on the insider threats organizations face today.

First off, and not surprising to those of us who focus on this space, organizations are experiencing **more data loss incidents than in years prior**, and it's a trend that continues despite investment in traditional data loss tools by virtually all surveyed companies. The second major finding is that the theft or leakage of an organization's source code (ranked in the top three most valuable data types) poses a particularly serious risk that can impact companies both financially and reputationally. **Source code exfiltration remains outside the view of traditional data loss tools, underscoring the criticality of the need for modern data protection solutions in the enterprise**.

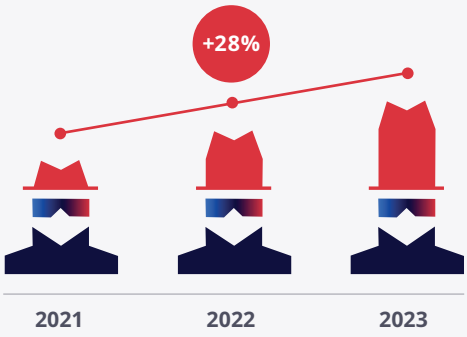
Finally, and again no surprise, **organizations of all sizes are concerned about the risks created by artificial intelligence tools**. In particular, the data sets required to fuel machine learning models represent significant risks as often well-meaning insiders push that data outside organizations to train the models. This is a whole new threat for which security teams are now responsible. Our mission at Mimecast is to secure human risk while protecting employee collaboration. That means encouraging teams to share data freely, knowing that they have a layer of security around that sharing. The Data Exposure Report helps our organization – and your organization – better understand the risks that come from today's innovative, data-sharing cultures.

TL;DR — Key Findings

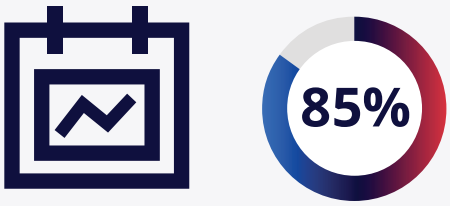
Data loss from insiders continues to pose a growing threat to security, with emerging technologies such as AI and generative AI (GenAI) only compounding the issue, indicating swift action is needed. Cybersecurity teams are demanding improvements in technology and training to tackle these issues and to ensure compliance with data security laws and regulations. There is an urgent need to prevent insider-driven data loss – to avoid damage to the company's reputation, competitiveness, and employee well-being, as well as their financial position.

KEY FINDING #1

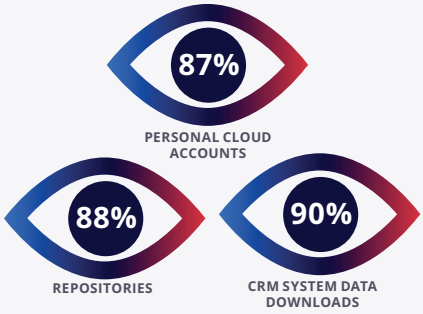
Companies need to improve their visibility and risk posture, as insider-driven data events continue to be a challenge, despite most having a traditional DLP solution in place.



There has been an increase of 28% in the average number of monthly **insider-driven data exposure, loss, leak, and theft events** – from 2021 to today



85% of cybersecurity leaders expect **data loss from insider events** to increase in the next 12 months

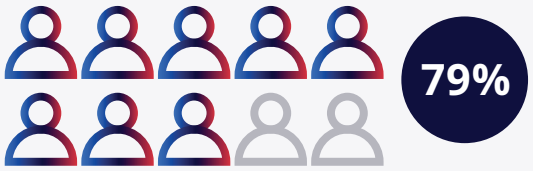


The majority of respondents state they need **more visibility** into source code sent to repositories (88%), files sent to personal cloud accounts (87%), and customer relationship management [CRM] system data downloads (90%)

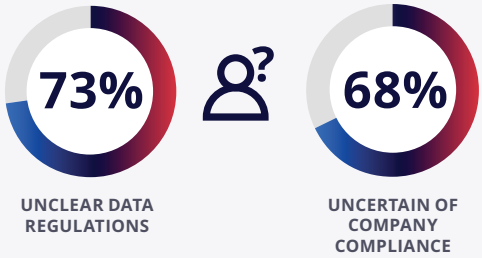
While most companies (99%) have data protection solutions in place, **these solutions are not mitigating data loss from insiders,** as 78% of cybersecurity leaders admit they have still had sensitive data breached/leaked/exposed

KEY FINDING #2

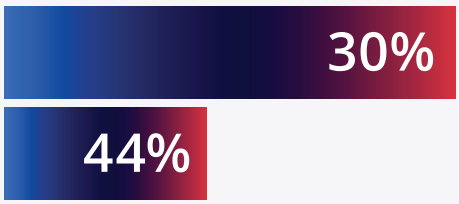
A shortage of cybersecurity skills creates a black hole for IP loss.



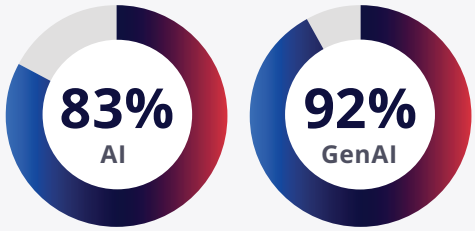
Over seven in ten surveyed cybersecurity leaders (79%) believe their cybersecurity team has a **shortage of skilled workers**



Seven in ten (73%) cybersecurity leaders agree that **data regulations are too unclear to adhere to**, while two-thirds (68%) state they're **not fully confident their company is complying** with new data protection laws



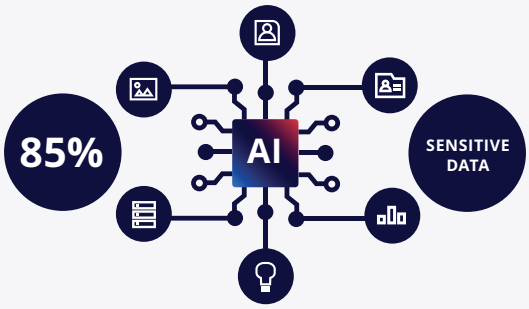
The vast majority believe that their company's **data security training requires improvement (98%)**, with over four in ten **(44%) stating it requires a complete overhaul**



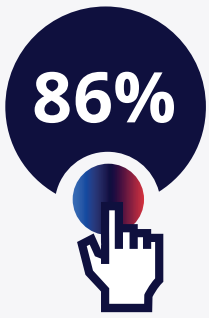
Cybersecurity leaders are looking to **AI (83%)** and **GenAI (92%)** to fill the cybersecurity skills gap

KEY FINDING #3

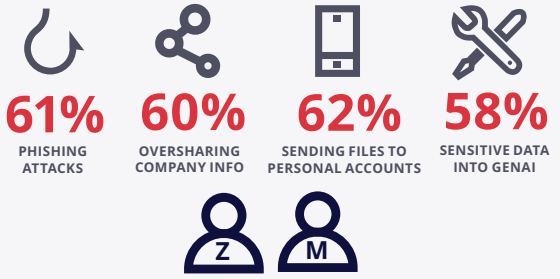
Emerging technologies and distinct employee types are creating unique risks to data security.



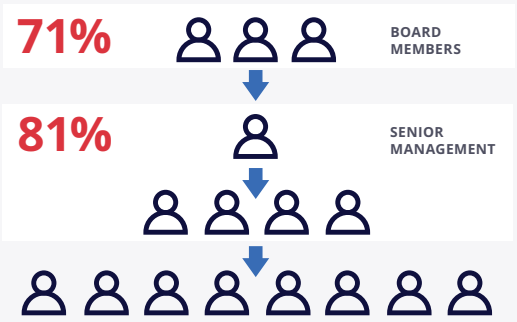
85% of cybersecurity leaders are concerned that their company's **sensitive data is increasingly vulnerable to new AI technologies**



86% of cybersecurity leaders worry that **employees may put sensitive data** into GenAI that will be found by competitors



Risks can also vary by employee type, with companies more concerned about **data security breaches from Generation Z and Millennials** falling victim to phishing attacks (61%), oversharing company information online (60%), sending company files/data to personal accounts/ devices (62%), and putting sensitive data into GenAI tools (58%)

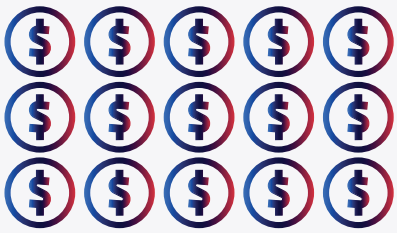


Respondents believe senior management (81%) and board members (71%) pose the **greatest risk to their company's data security**, likely due to having wide-reaching access to the most sensitive data

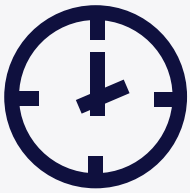
KEY FINDING #4

Data loss from insiders drains time, money, and security teams.

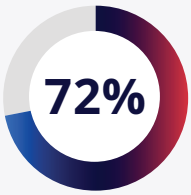
15M



Insider-driven data exposure, loss, leak, and theft events can have vast **financial repercussions**, with cybersecurity leaders estimating that a single event would cost their company $15 million, on average



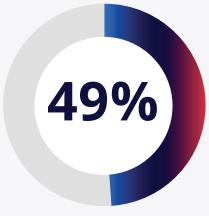
3h



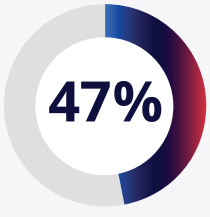
There are also costs to security teams, who are **wasting time with limited resources**:

An average of 3 hours per day is spent investigating insider-driven data events

72% of cybersecurity leaders are worried they could lose their job from an unaddressed insider breach



DETECT/RESPOND TO DATA EXFILTRATION



MORE CENTRALIZED VISIBILITY

Companies are planning to **consolidate their data protection solutions** in 2024 to improve their ability to detect and respond to data exfiltration (49%) and to give them more centralized visibility (47%)

42%

SPEED/EASE

39%

VISIBILITY

38%

INTEGRATION

To be effective, companies believe that **data protection solutions** should offer speed and ease of investigation (42%), visibility into file contents and metadata (39%), and should be able to integrate with other tech solutions (38%)

Objective of the Annual Data Exposure Report: 2024

In past Annual Data Exposure Reports, the research has focused on key drivers of data loss from insiders and challenges to building and running insider threat technologies, training, and programs. In the 2024 edition, we wanted to understand how companies are managing insider-driven data loss in light of changing workforce trends and generative AI.

To explore this, we surveyed 700 respondents – consisting of cybersecurity leaders, cybersecurity managers, and cybersecurity practitioners – from U.S. companies with 500 or more employees from a range of public and private sectors.

Part 1
Introduction

2024 was another difficult year for cybersecurity teams, with insider-driven data loss persisting at the core of a complex threat landscape. Given the long-reaching implications of these events, teams must act proactively to ensure the security of their IP.

Insider threats occur when sensitive corporate data — IP, digital assets, trade secrets, source code, crown jewels — moves to untrusted destinations like personal devices, email, or cloud applications due to the behaviors of insiders, malicious or accidental. Such data movement presents considerable competitive, financial, privacy, and compliance risks to the company.

Data loss from insiders remains a pervasive problem to solve, with companies experiencing 28% increase in average monthly number of insider-driven data events from 2021 to today. While companies continue to check the data protection box with traditional DLP solutions, the unabated rise in insider events signals that these legacy tools aren't cutting it. In an ever-evolving digital world, there's a pressing need to invest in more *effective* data protection solutions that can handle today's velocity and complexity of data risk.

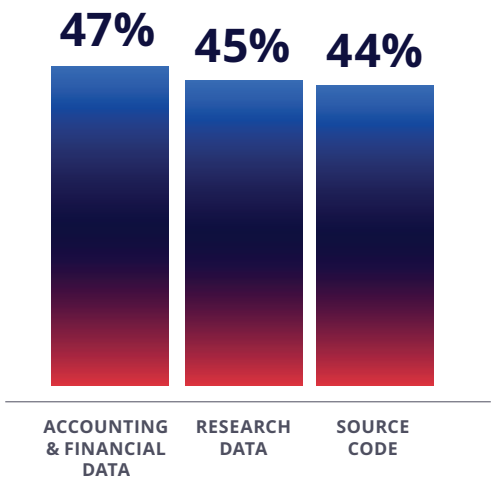
A shifting workforce also poses new challenges to data protection, with the cybersecurity skills gap adding pressure on companies to retain their best talent while ensuring employee time is optimized. This balancing act is exacerbated by the time demands of investigating insider-driven data events, and the serious impacts of missing them, especially as we continue to see a failure to mitigate these incidents. In a year where AI has become mainstream, most companies are looking to leverage these advancements to maximize team impact, and this is no different in security. Still, while AI tools are blazing a new trail, they pose a significant threat to data security.

In this year's report, we take a closer look at workforce challenges and threats from AI in the context of insider threats and shed light on the need for effective data protection solutions and high-quality data security training.

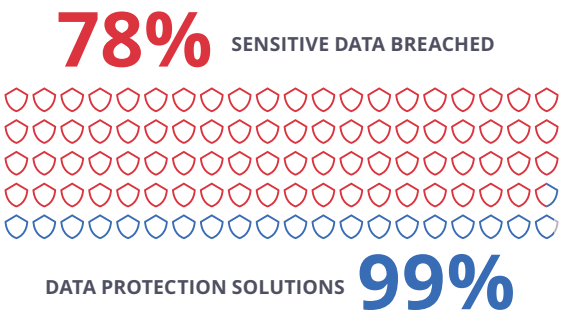
Part 2
Current State of Data Loss

Companies need to improve their visibility and risk posture as current data protection solutions are proving ineffective in mitigating data loss

TOP THREE MOST VALUABLE TYPES OF DATA



Which of the following data types are the most valuable to your company? [700] Combination of responses ranked first, second and third, showing top three answers only.



While most companies (99%) have data protection solutions in place, **these solutions are not mitigating data loss from insiders**, as 78% of cybersecurity leaders admit they've still had sensitive data breached/leaked/exposed

Data is at the core of any company, and in this report, it's well-evidenced that not only the regulated and classified data is important, but all of a company's IP needs protecting. A company's intellectual property and their ability to harness and interpret data enables them to adapt to ever-changing market conditions, enhance innovation, and ultimately drive growth and profitability.

Nevertheless, most companies deem some data of highest value, with our surveyed cybersecurity respondents placing accounting and financial data (47%), research data (45%), and source code (44%) among their top three most valuable data types.

Companies are trying to protect their valuable data as almost all companies surveyed (99%) have data protection solutions in place. However, the unfortunate truth is that these solutions are failing, as over three-quarters (78%) of cybersecurity leaders admit their company has still had data breached, leaked, or exposed, despite having a data protection solution in place. Hence, 87% of cybersecurity leaders feel their company's data protection solution needs improving.

Exfiltration of data can happen in various ways, with personal cloud accounts (42%), customer relationship management systems (40%), and files sent to personal email addresses (39%) ranked as the top three methods that pose the greatest risk. Detecting and mitigating data loss from insider threats necessitates a clear understanding of who is moving or altering

24 insider-driven data exposure, loss, leak, and theft events experienced a month, on average

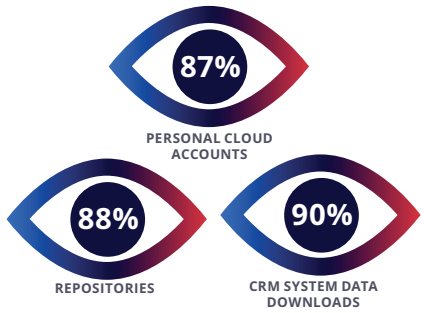
the data, where it originates, and where it is going; yet the vast majority of respondents stated that their company needs better visibility into these areas. A lack of visibility undermines a company's ability to proactively protect its data, as it is unable to monitor compliance with regulations and cannot effectively detect suspicious use and movement of its most important IP.

The majority (88%) of respondents believe their company needs more visibility into source code sent to repositories, while 28% rank it among the top three methods that pose the greatest exfiltration risk. Source code poses a unique risk to cybersecurity, as its theft or leakage can result in unauthorized access, lost competitive edge due to stolen IP, or intentionally introduced vulnerabilities, all of which put companies at serious risk.

This lack of visibility to unknown risks across many types of vectors for file movement is a key contributor to the high number of insider-driven data exposure, loss, leak, and theft events respondents estimate their company experiences each month. Since 2021, there has been a 28% average increase in the number of exfiltration events. This illustrates a persisting issue in effectively addressing insider-driven data loss, regardless of having a traditional data protection solution in place.

PROPORTION OF INTENTIONAL VS UNINTENTIONAL INSIDER-DRIVEN DATA EXPOSURE, LOSS, LEAK, AND THEFT EVENTS EXPERIENCED IN THE LAST 12 MONTHS

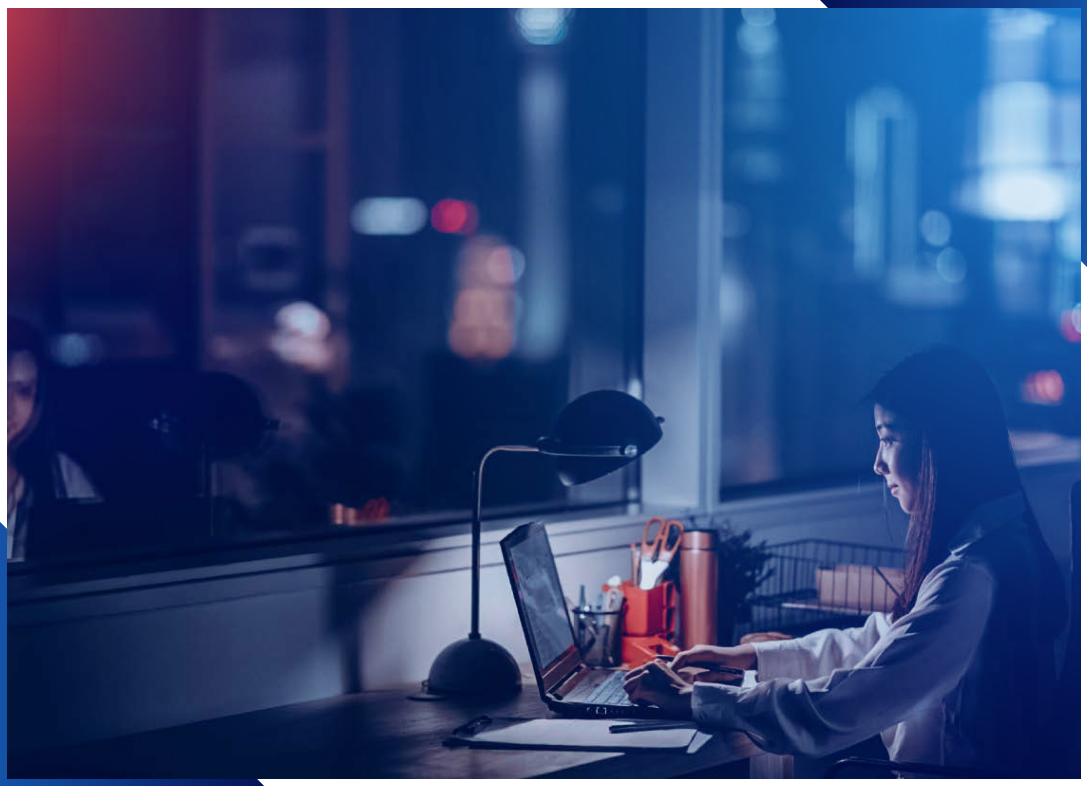
What proportion of insider-driven data exposure, loss, leak, and theft events in the last 12 months do you estimate were intentional vs. unintentional in your company? [700]. Showing the average % only



The majority of respondents state they need **more visibility** into source code sent to repositories (88%), files sent to personal cloud accounts (87%), and customer relationship management [CRM] system data downloads (90%)

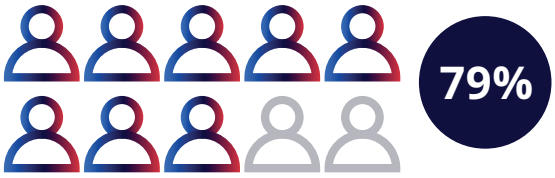
Threats can arise from both intentional and unintentional actions by individuals with access to sensitive information, and our research suggests there is a slightly greater amount of intentional events occurring. Considering this spread of unintentional vs. intentional events, it's even more critical that organizations utilize modern data protection solutions to reduce the burden of lower risk, unintentional events on security teams. In doing so, teams can free up the time and resources needed to investigate intentional events. This makes it very difficult for companies to prioritize and monitor threats, as they come from different directions – an issue that could be better remedied with a holistic approach.

Insider-driven data events are not going away any time soon as **73% of respondents believe these events will increase in their company in the next 12 months**. Surveyed cybersecurity leaders are more likely to anticipate this increase, compared to cybersecurity practitioners (85% vs. 61%), which is likely due to the fuller picture they have of the risks their company faces, indicating significant threat of insider events and the urgent need for better protection.

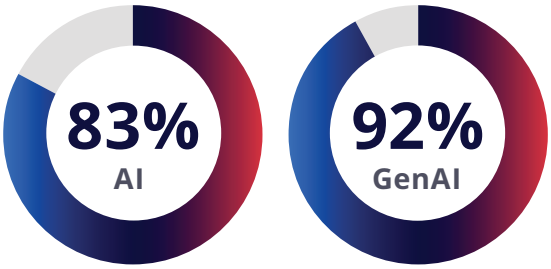


Part 3
Current State of the Workforce

A shortage of cybersecurity skills creates a black hole for IP loss



Around four in five cybersecurity leaders believe their teams have a **shortage of skilled workers**



92% agree that "My company is using GenAI to make up for a lack of cybersecurity skills"

The state of the workforce plays a crucial role in a company's ability to keep data secure, including the ability to prevent and respond to insider-driven data incidents. Gartner predicts that by 2025, lack of talent or human failure will be responsible for over half of significant cyber incidents.[1]

Our research shows that around four in five (79%) cybersecurity leaders believe their cybersecurity team has a shortage of skilled workers. This opens companies up to gaps in implementing and maintaining robust security measures to protect them from insider threats and could be a catalyst for the continued issue of data loss.

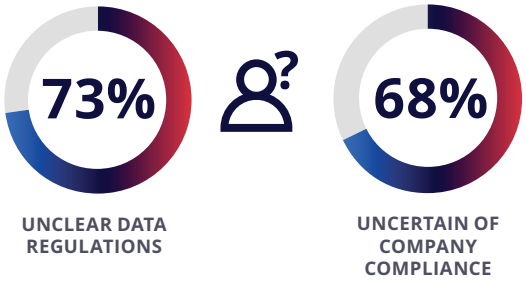
With increasing demand for qualified cybersecurity professionals to address evolving threats, existing personnel must use their time wisely. Our research found that teams spend an average of 3 hours per day investigating potential insider-driven data events, consuming a significant portion of their working day What's worse, 87% of cybersecurity leaders believe investigation time for data incidents is increasing. This adds undue pressure on cybersecurity teams, with under-staffed teams spending valuable time on tedious tasks that could be resolved through automation and improved signal-to-noise ratio via a robust data protection solution.

Fortunately, cybersecurity leaders recognize the critical need to alleviate the burden on their team, with many companies looking to AI (83%), and even more so GenAI (92%), to fill the skills gap. While this can bring opportunities, we will see in part 4 that it can also bring about new threats.

Over seven in ten (73%) of cybersecurity leaders are finding data regulations too unclear to adhere to, which could be why two-thirds (68%) are not fully confident that their company is complying with new data protection laws. Regulations might be influencing technology and platform selection for companies striving to achieve compliance goals, but unclear guidelines make it difficult to know what is appropriate. Auditors and cybersecurity teams need to work together to meet compliance requirements in a way that aligns to the needs of their company.

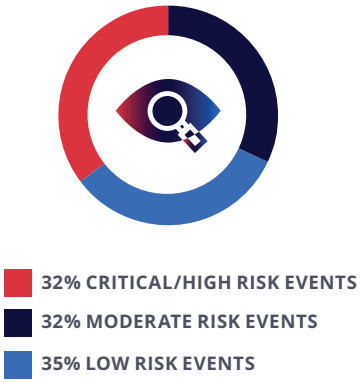
Our analysis of risk severity shows a roughly even spread of insider-driven data events being critical/high-risk (35%), moderate risk (32%), and low risk (32%). These differing levels of severity make detection and response prioritization difficult, as teams are constantly having to pivot from common threats to critical events that demand thorough investigation. This deters security teams from maximizing their focus and efficiency, resulting in significant burden on teams that are already strapped for time and headcount resources.

Targeted, responsive data security training can address lower-level risk events and give teams time back to investigate high-risk events, as employees are often the first line of defense against data loss. Aligned with our 2023 research, data security training is most likely to be conducted weekly (2024: 34%, 2023: 30%). However, there has been a steady increase over time in the proportion of companies conducting it daily, from 11% in 2021 to 15% in 2023, and now 27% in 2024. This increase in frequency could be in response to the urgent need to tackle the problem that has shown no signs of improvement over the last few years.



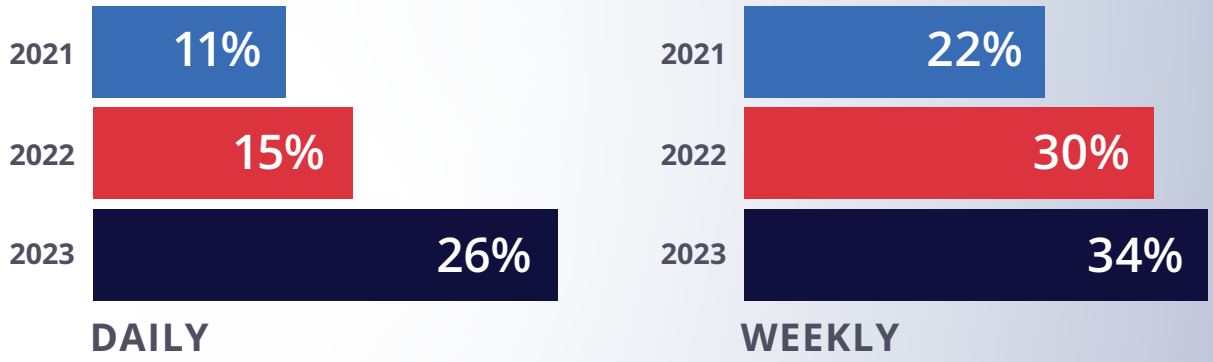
68% cybersecurity leaders are **not fully confident that their company is complying** with new data protection laws

TYPE OF INSIDER-DRIVEN DATA EXPOSURE, LOSS, LEAK, AND THEFT EVENTS BEING INVESTIGATED



Approximately, what proportion of the insider-driven data exposure, loss, leak, and theft events that are investigated fit into the following severity types for your company? Showing the average % [700]

FREQUENCY OF EMPLOYEE DATA SECURITY TRAINING



How often is employee data security training (training specifically oriented around the handling of data) conducted at your company? Not showing all answer options [700]

Companies conducting training daily experience fewer insider-driven data events a month than those who conduct it quarterly (23 vs. 28, on average). However, nearly all (98%) companies, regardless of how often they conduct training, believe it requires improvement. In fact, those who conduct it daily are more likely to feel a complete overhaul is needed, compared to those who conduct it quarterly (42% vs. 26%). This suggests that while regular data security training can provide scalability for companies to address the varying severity of insider-driven data events, its effectiveness in thwarting risk hinges on its quality. Learn more about **Mimecast's security awareness training** to reduce risk and protect your company from the evolving threat landscape posed by insiders.

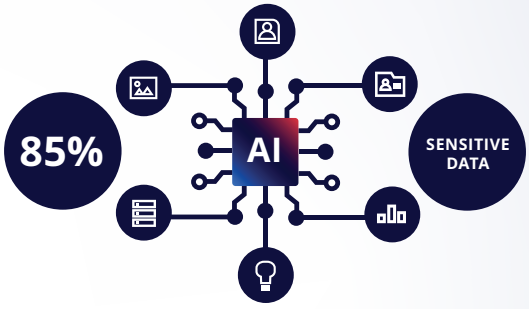
Part 4
Accelerators of Risk to Data

Emerging technologies and varying employee types are creating risks to data security

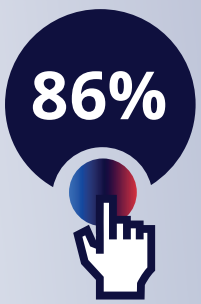
Emerging technology

Artificial Intelligence (AI) can open new doors for cybersecurity teams, helping them to automate detection and response so that they can focus on higher-level strategic tasks. This optimizes security operations, allowing cybersecurity personnel to work more effectively, and helping to close the skills gap. Still, AI is not a one-to-one replacement for team talent, and if not used appropriately, it can pose serious risks, with 86% of surveyed cybersecurity leaders admitting that AI tools put their company at risk of data exfiltration.

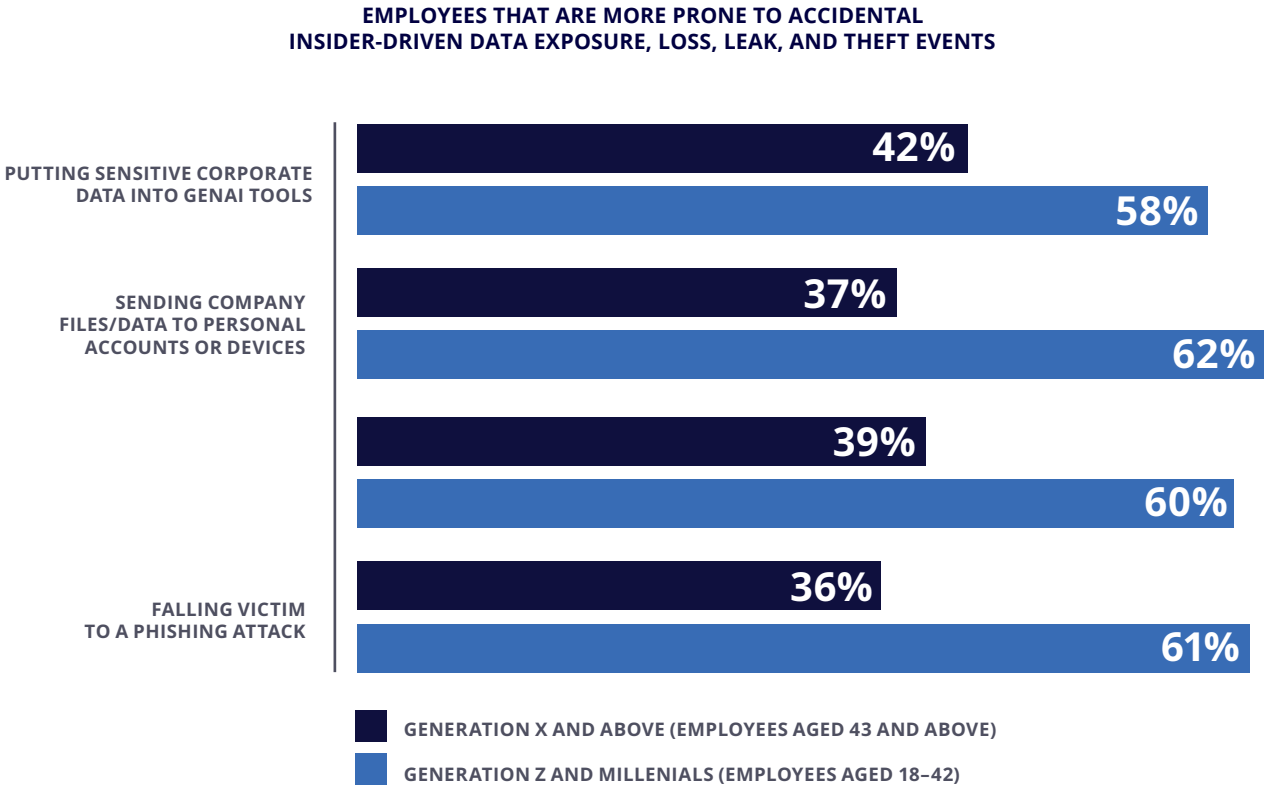
The risk level intensifies when we consider high-value data, with 85% of cybersecurity leaders expressing concern that their company's sensitive data is increasingly vulnerable to new AI technologies. Confidential data or source code put into an AI tool may train the model and inform future outputs for untrusted users. It may also deliver malicious outputs. This puts compliance obligations and intellectual property at risk, and is a serious concern for cybersecurity leaders, with 86% of those surveyed fearful that employees may put sensitive data into GenAI that will be found by competitors.



85% of cybersecurity leaders are concerned that their company's **sensitive data is increasingly vulnerable to new AI technologies**



86% of cybersecurity leaders worry that **employees may put sensitive data** into GenAI that will be found by competitors



Which of the following employees do you think are most prone to accidental insider-driven data exposure, loss, leak, and theft events in your company? [700]

Traditional DLP solutions are failing to expose this risk, as 90% of companies using DLP still require more visibility into data being pasted into Generative AI tools. Providing clear guidelines on the use of AI, such as an **Acceptable Use Policy**, may increase the likelihood that employees will utilize it responsibly, so it's encouraging that 78% have a policy in place around proper use for GenAI at work – but are their workforces complying?

Our research suggests they're not, as **87% of respondents express concerns that employees aren't adhering to the policy their company has in place**. Employees are the gateway to AI security threats and failing to comply could result in some of the risks we saw previously around data exfiltration and sensitive data being found by competitors. This necessitates a modern method of exfiltration detection with a wide range of response controls – from blocking unacceptable activity to situational and responsive training.

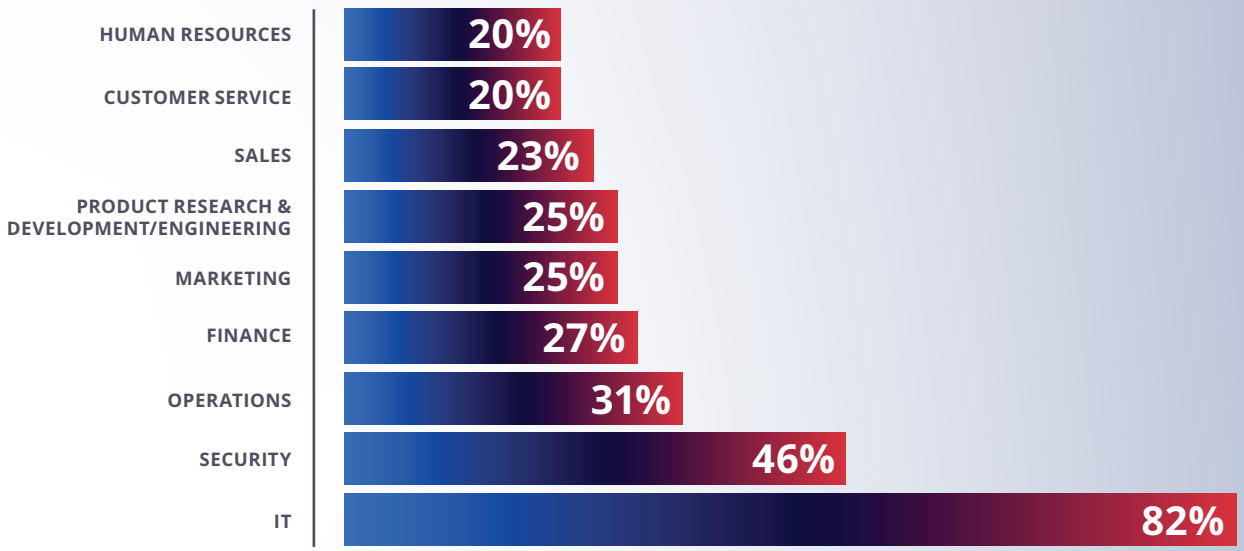
Employee Types

It's not just technology that is posing a threat to company data; varying employee demographics also play a part. Surveyed respondents believe Generation Z and Millennials are more likely than Generations X and above to send company files to their personal accounts/devices, fall victim to a phishing attack, overshare company information online, and put sensitive corporate data into GenAI tools. This may be because they are more actively involved in the digital world, seeing it as an extension of their blurred working and personal lives; and with the BLS predicting that the millennial labor force will see the largest increase in size over the next few years2, the risk level these employees bring to companies is only likely to increase further.

Risk is also driven by employee role and level, with **senior management (81%) and board members (71%)** ranked as the top two most likely groups to risk their company's data security. This may be because they have access to sensitive information and higher-level permissions, which inherently makes any type of data leak from this demographic much more serious. For these groups, training and education are particularly important to ensure they are acting securely and setting a tone of security and responsibility for the rest of the business.

When it comes to departmental risk, it's no surprise that IT (82%) and Security (46%) are most likely to be ranked among the top three departments that pose the greatest security risk, given their higher levels of access. However, across other departments the risk level is fairly distributed, suggesting that all employees have the potential to put data in jeopardy.

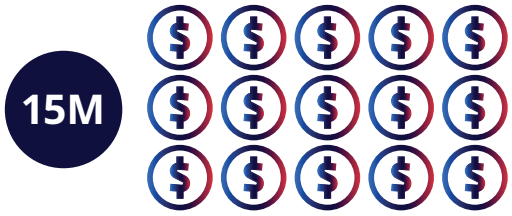
DEPARTMENTS POSING THE GREATEST RISK TO DATA SECURITY



Which of the following departments pose the greatest risk to data security in your company?
Combination of responses ranked first, second, and third [700]

Part 5
Impact of Insider-driven Data Loss

Data loss impacts time, money, and employees

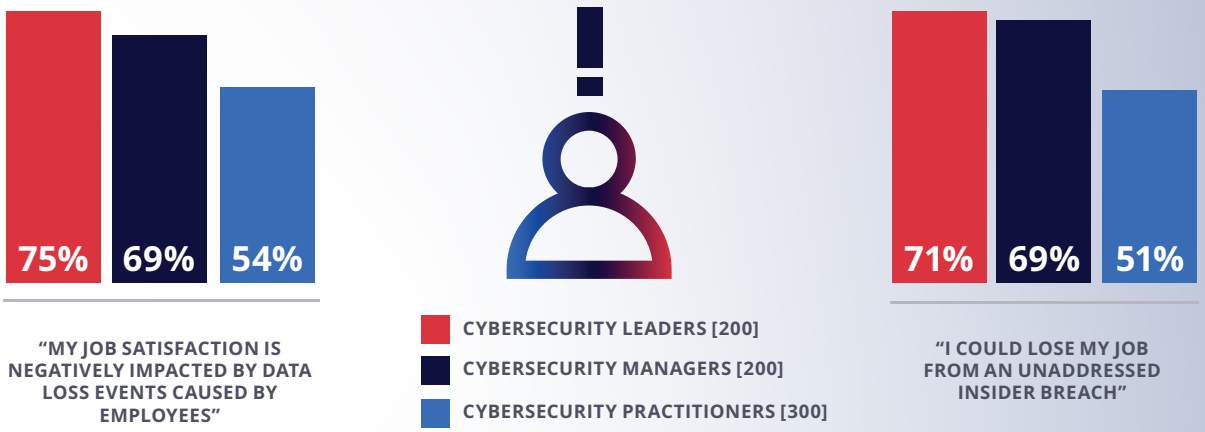


Cybersecurity leaders estimate that insider-driven events would cost their company $15 million, on average

Insider-driven data events have multifaceted repercussions for companies. The financial impact is substantial, with surveyed cybersecurity leaders **estimating them to cost their company $15 million, on average**. This has grave consequences for fiscal stability, operational resilience, and the overall ability to thrive in an increasingly difficult market.

The impact of data loss from insiders extends far beyond finances, including the loss of talent. The majority (87%) of respondents admit their company has terminated employees within the last 12 months as a result of insider-driven data events, with an average of 9 employees let go.

IMPACT TO JOB SATISFACTION & JOB LOSS FROM DATA LOSS EVENTS & INSIDER BREACHES



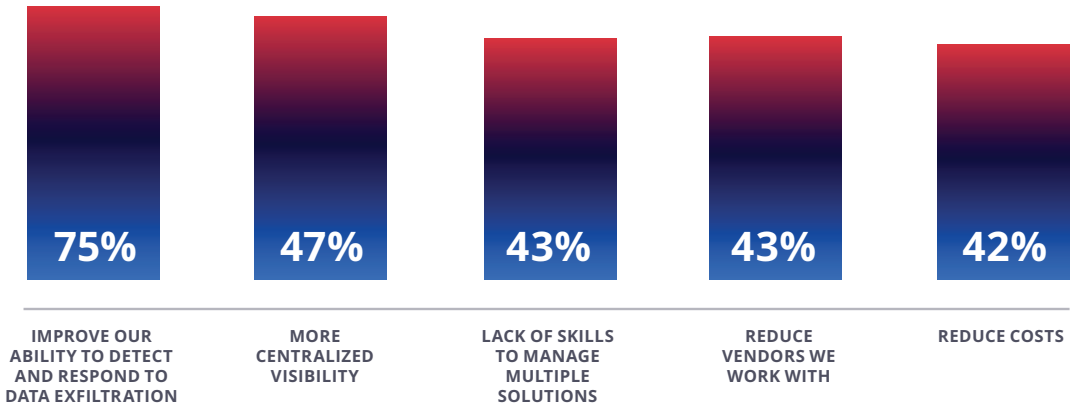
To what extent do you agree or disagree with the following statements? Comments show in graph.
Showing 'agree' only. Split by respondent type [Base sizes in chart]

Employees are one of the biggest risks to companies, especially when they depart, with **eight in ten (80%) cybersecurity leaders admitting that departing employees take valuable IP when they leave**. This could be happening even more than they realize, with seven in ten (70%) saying their company is not always aware of when sensitive data is taken by departing employees. The significant gaps in the visibility of employee behaviors puts companies at risk of reputational damage and losing their competitive edge in the market.

Employee morale has taken a knock too, with three quarters (75%) of cybersecurity leaders seeing their job satisfaction negatively impacted by data loss events caused by employees. A similar proportion (72%) are also fearful they could lose their job from an unaddressed insider breach, which is the last thing cybersecurity teams need amidst a skills shortage. Morale and fear are felt more among leaders than among managers and practitioners, which is likely due to their higher level of accountability and responsibility when things go wrong. With insider-driven data events on the rise, leaders need to have data protection tools and strategies they can rely on to mitigate risk, in order to improve morale and reduce fear around job loss.

Employees are one of the biggest risks to companies, even when they depart, with **eight in ten (80%) cybersecurity leaders admitting that departing employees take valuable IP with them when they leave**.

TOP FIVE DRIVERS TO CONSOLIDATING DATA PROTECTION SOLUTIONS



Which of the following are drivers to consolidating your company's data protection into fewer solutions in 2024?
Combination of responses ranked first, second, and third. Not showing all answer options.
Only shown to those with a data protection solution in place. [693]

Despite nearly all (99%) respondents stating that their company has data protection solution(s) in place, 78% of surveyed cybersecurity leaders admit that they have still had sensitive data breached, leaked, or exposed. This makes it no surprise that 87% of cybersecurity leaders admit that their current solution needs improvement. To make matters worse, around nine in ten (88%) are finding their solution more work than anticipated, possibly due to it being complex and resource intensive.

Clearly, traditional data protection capabilities need to evolve to meet existing cybersecurity landscape demands and alleviate burden on already over-stretched cybersecurity teams. Companies need solutions that provide visibility, context, and controls to prioritize threats and drive a secure workforce.

TOP FOUR MOST IMPORTANT FACTORS FOR AN EFFECTIVE DATA PROTECTION SOLUTION

42%

SPEED AND EASE OF INVESTIGATION

38%

ABILITY TO INTEGRATE WITH OTHER TECH SOLUTIONS

39%

LEVEL OF VISIBILITY INTO FILE CONTENTS AND METADATA

38%

EASE OF DEPLOYMENT

Which of the following factors do you believe are most important to determine if a Data Protection solution will be effective? Combination of responses ranked first, second, and third

As we look more closely into the solutions companies have in place, 87% are using traditional Data Loss Prevention (DLP). However, this policy-based, blocking-first solution isn't an effective approach to the problem, given the high number of events those using it still experience. Via tagging and endpoint control, DLP can offer benefits in detecting and preventing data exfiltration and, when used and maintained vigorously, can support compliance with standards such as HIPAA, PCI-DSS, and GDPR; **but it relies on meticulously identifying, classifying, and blocking all real-time data movement, an impossible task when data is being created and legitimately used and changed every second.**

All surveyed companies that have a data protection solution are planning to consolidate in 2024. Security teams are looking for improvements in detection and response to data exfiltration (49%), more centralized visibility (47%), don't have the skills to manage multiple solutions (43%), and want to reduce costs (42%). Gaining efficiencies and more visibility require a solution created for the modern, collaborative business, but attempting to over-compromise on price could actually cost more in the long run – not just from a financial standpoint, but also in terms of reputation.

With traditional data protection solutions currently failing companies, what areas are they hoping to address? Speed and ease of investigation (42%), visibility (39%), integration (38%), and deployment (38%) are among the most important factors. This will help to reduce the number of insider-driven data events companies experience and relieve the stress and burden on cybersecurity personnel.

Part 6
Conclusion

Data loss from insiders is becoming an increasingly urgent problem for companies to solve. Workforce trends and emerging technologies are accelerating the risk to data and adding to the complexity of the issue, with insider-driven data events absorbing large chunks of time for under-skilled and under-resourced cybersecurity teams that could be allocated to higher-level strategic tasks. **While companies are turning to AI and GenAI to plug the skills gap, these tools are not a replacement for team talent and can open the door to more risk.**

This threat cannot be ignored, with compliance obligations and IP at greater risk from employees inputting sensitive data into GenAI tools. We saw that many companies have guidelines for employees to use GenAI responsibly, but with so many fears that employees are skirting the policies in place, the risk remains high. Greater visibility is needed so that companies have sight on data being copied into GenAI tools to identify and remediate risks before it's too late. This makes it essential to have an effective data protection solution, but our research has shown that most are failing.

The majority of companies we surveyed are using legacy DLP, yet still experience a high number of insider-driven data events, illuminating the fact that traditional data security tools are failing to meet current needs. Today's risks are driven by AI and Generative AI, the way employees work, and the proliferation of cloud applications. The types of data that are most important to a company's value are no longer easily immobile, easily tagged, and restricted. Source code, roadmaps, and financial data live and move across various applications and are touched by many employees on an hourly basis, making traditional data security tools ineffective in today's digital world.

The constant fine-tuning required by legacy tools drains time and money in a workforce that is already stretched thin. Instead, companies need a solution that can quickly see and stop threats in one platform. This makes a holistic response strategy that uses automated training to eliminate human response to low-risk data events and block unacceptable activity, the ideal solution.

With the consolidation of data protection into fewer solutions being a key objective for companies in 2024, **Incydr** could be the answer to reducing security product sprawl. **Incydr** helps companies quickly see and stop data leaks and theft in one platform, eliminating the need for traditional DLP, CASB, and UEBA in most cases, across technology, manufacturing, life science, and business service industries.

Part 7
Methodology

Code42, now a Mimecast company, commissioned the independent market research agency Vanson Bourne to conduct the Data Exposure Research. The 2024 study surveyed 700 respondents (300 cybersecurity practitioners, 200 cybersecurity managers, and 200 cybersecurity leaders) from companies in the US from December 2023 to January 2024. These companies had 500 or more employees and were from a range of public and private sectors, including automotive and aerospace/manufacturing, business and professional services, energy, oil/gas and utilities, technology, and pharmaceutical and life sciences/biotechnology, among other sectors.

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 now retired 2023 and 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 2024 wording.

About Mimecast

Mimecast is an AI-powered, API-enabled connected Human Risk Management platform, purpose-built to protect organizations from the spectrum of cyber threats. Integrating cutting-edge technology with human-centric pathways, our platform enhances visibility and provides strategic insight that enables decisive action and empowers businesses to protect their collaborative environments, safeguard their critical data and actively engage employees in reducing risk and enhancing productivity. More than 42,000 businesses worldwide trust Mimecast to help them keep ahead of the ever-evolving threat landscape. From insider risk to external threats, with Mimecast customers get more. More visibility. More insight. More agility. More security.