Annual Data Exposure Report

LIFE SCIENCES SECTOR

2024

TL;DR – Key Findings

Insider-driven data loss events remain a growing security threat, made worse by emerging technologies like AI and GenAI, despite increased DLP investment. Leaked trade secrets or critical intellectual property (IP) – research data, customer lists, pricing decks, formulary plans, trial data, and source code – can derail Life Sciences organizations. Data is the lifeblood of cutting-edge companies in this sector, and any leak or loss can result in lost opportunities, reputational damage, and even potential HIPAA violations.

Given the critical nature of safeguarding IP, security leaders and teams must have robust protections in place to tackle insider threats. The Life Sciences Cohort of cybersecurity respondents in the 2024 Annual Data Exposure Report (DER) revealed the following:

73%

73% of respondents are **using AI to fill the skills gap.**

84%

84% of cybersecurity managers **believe they are short-skilled.**

78%

78% of companies report **rising data incident investigation times annually.**

Top 3 most valuable data types ranked by Life Sciences industry respondents:

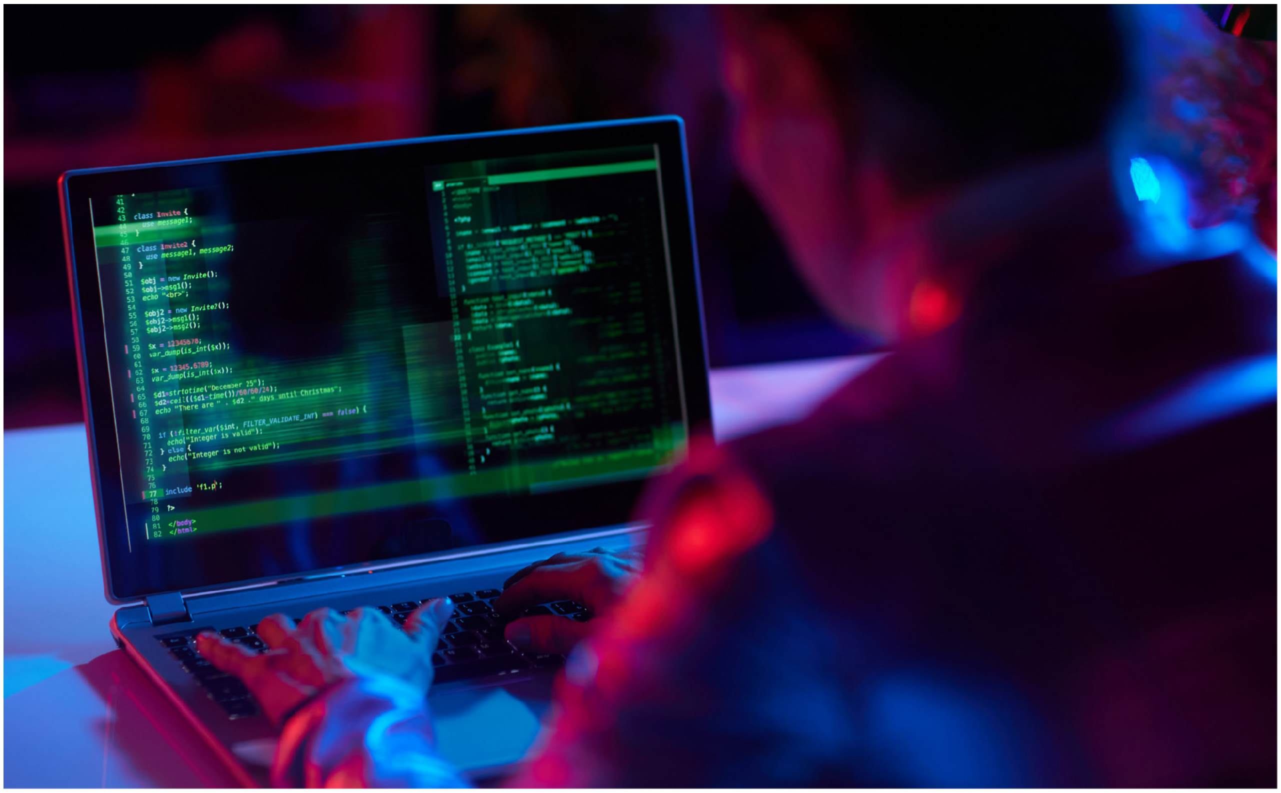
Accounting and financial data	Research data	Source code
47%	45%	44%

Introduction

“Despite most organizations having a traditional data loss protection (DLP) tool in place, insider threats remain a critical source of data leak across all industries. However, the impact of these threats **is particularly felt in the Life Sciences sector**, where organizations within the medical device, biotech, and pharmaceutical industries are required to keep intellectual property secure.

These organizations are entrusted with a wide range of confidential data, including patient records, proprietary research findings, product blueprints, and manufacturing protocols. A data leak or loss event could result in significant losses, with **insider-driven incidents estimated to cost Life Sciences organizations around $14M**. Safeguarding these assets against unauthorized access is vital for Life Sciences organizations to maintain their competitive advantage and ensure uninterrupted business operations.

The consequences of failing to protect against these threats extend far beyond financial losses, reputational damage, and legal battles; they jeopardize the very foundation of patient trust and can lead to an untold loss of business opportunities. Recently, pharmaceutical giant **Pfizer filed a high-profile lawsuit** against its long-time employee who allegedly stole numerous confidential documents as she prepared to join a competitor. The lawsuit claimed that the employee breached her confidentiality agreement by uploading over 12,000 proprietary files, including those related to its COVID-19 vaccine, to her personal accounts and devices from her company- issued laptop. As they had spent $9.4 billion on research and development in 2020, a trade secret leak of this magnitude would not only jeopardize their competitive position but would also disrupt their time to market.”



In another case of trade secret theft within the biopharma sector, **former Genentech employees – Xanthe Lam, a principal scientist, and her husband Allen Lam – plead guilty** to conspiring to steal proprietary information that would benefit competitors. The stolen data was related to several cancer drugs produced by Genentech, including Rituxan, Herceptin, Avastin, and a cystic fibrosis treatment. This intellectual property was shared with JHL Biotech, now known as Eden Biologics. The US Department of Justice also targeted other involved parties, including JHL Biotech co-founders Racho Jordanov and Rose Lin, who were indicted by a federal grand jury in San Francisco. Both are former Genentech employees and allegedly initiated the plan to steal trade secrets as early as 2008, later enlisting the Lams in 2009 and establishing JHL in 2011. These individuals allegedly utilized thousands of documents to expedite product development processes by cutting corners and reducing costs.

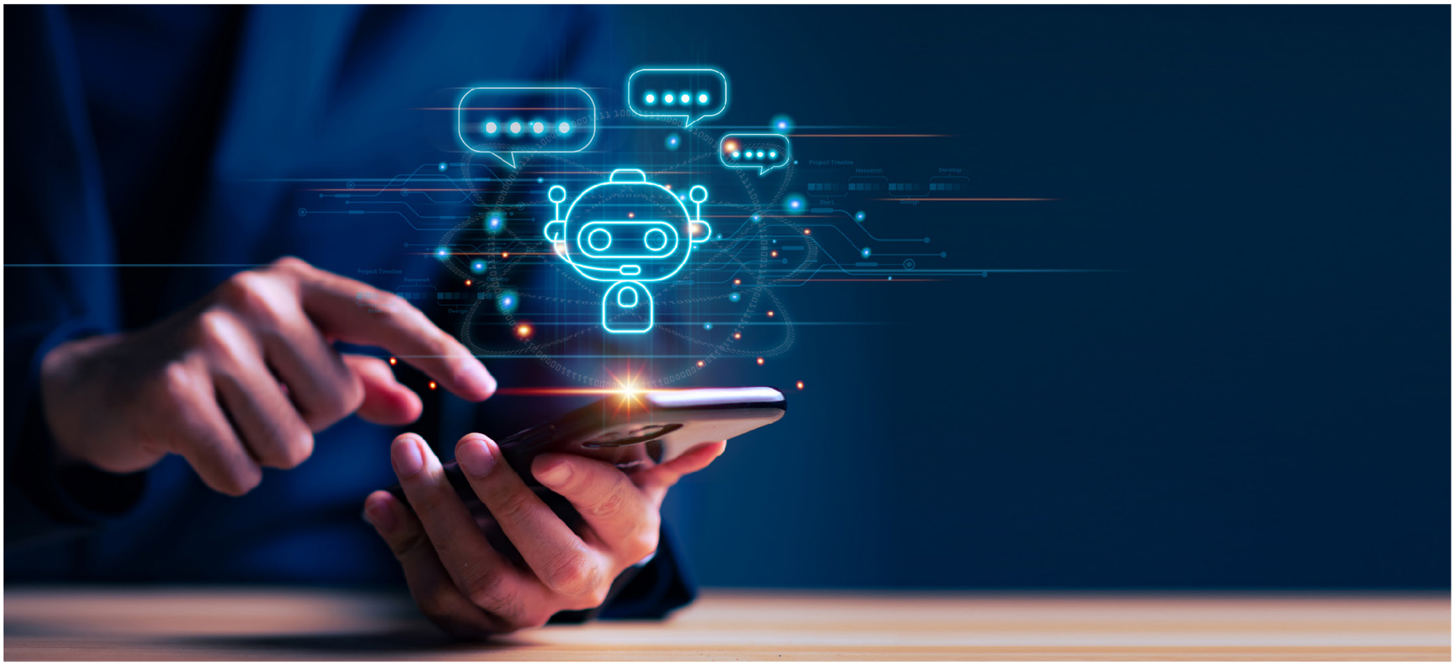
Such incidents illuminate the glaring vulnerability that Life Sciences organizations face, even for those with robust data protection controls in place. **To uphold customer trust, safeguard intellectual assets, and maintain their competitive advantages, these businesses must confront the challenge posed by insider-driven data loss.**

Life Sciences Industry is Leading the Pack in Using AI to Fill the Skills Gap

But most cybersecurity leaders acknowledge AI poses a risk to data security

Effective data protection, encompassing the prevention and mitigation of insider-driven data incidents, is heavily contingent on the workforce's state within a company. **As teams become further strapped for cybersecurity talent, the safety of corporate data hangs in the balance.** Artificial Intelligence (AI) and Generative AI (GenAI) are revolutionizing the future of work, allowing businesses to face the talent shortage head-on by optimizing the time of their skilled employees.

As 78% of companies in the Life Sciences sector have experienced an increase in time spent investigating data incidents year over year, these organizations have been spurred to adopt new AI tools at a rapidly increasing rate – surpassing other industries in a mission to continue innovating in the face of talent-shortage headwinds.



Which of the following data types are the most valuable to your company?

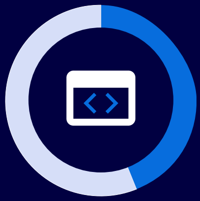
Combination of responses ranked first, second, and third, showing top three answers only

Accounting & financial data

47%

Research data

45%



Source code

44%

Cybersecurity Leaders Face Talent Shortage & AI Risks Despite Vulnerability Concerns

79%

79% believe that their cybersecurity team has a **shortage of skilled workers**

73%

73% **are using AI to fill the skills gap**

84%

84% believe their **sensitive data is increasingly vulnerable** to new AI technologies

86%

86% have admitted that the **usage of AI tools does put their company at risk** of data exfiltration

85%

85% have expressed concern that their company's **sensitive data is increasingly vulnerable** to new AI technologies

“This is especially concerning for businesses in the Life Sciences sector, whose sensitive data directly affects core operations. Survey respondents cite **accounting and financial data as the most valuable data type (47%), followed by research data (45%) and source code (44%).** Maintaining these specific data types is vital for Life Sciences businesses to remain competitive, as their loss would undoubtedly impact future business opportunities.”

“With that in mind, 83% of cybersecurity managers are looking to AI, and 92% to GenAI, specifically, to help them 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 can pose serious risks if policies are not in place to protect proprietary data.

- 79% of cybersecurity leaders believe that their **cybersecurity team has a shortage of skilled workers**. This creates gaps in implementing and maintaining robust security measures to protect from insider threats, and could also be a catalyst for continued data loss.
- 73% of Life Sciences respondents **are using AI to fill the skills gap** – more than companies in aerospace and the oil/gas/utilities industries; but that percentage is still less than that of consulting and business services companies.
- 84% of Life Sciences companies believe their **sensitive data is increasingly vulnerable to new AI technologies,** especially GenAI.
- 86% of surveyed cybersecurity leaders have admitted that the **usage of AI tools does put their company at risk of data exfiltration**.
- 85% of cybersecurity leaders have expressed concern that their company’s **sensitive data, including source code, is increasingly vulnerable to new AI technologies**.

Those in the Life Sciences know well the critical nature of adhering to regulations. However, ambiguous new policies around data protection are leaving teams scrambling to piece together sufficient protocols, evidenced by the fact that two-thirds of cybersecurity leaders are not fully confident that their company is complying with these new laws. Organizations aiming to meet compliance goals may choose certain technologies and platforms to adhere to regulations. However, vague guidelines can create challenges in determining the most suitable options. Collaboration between auditors and cybersecurity teams is essential to ensure compliance.”

How Can Life Sciences Organizations Minimize Insider Incidents?

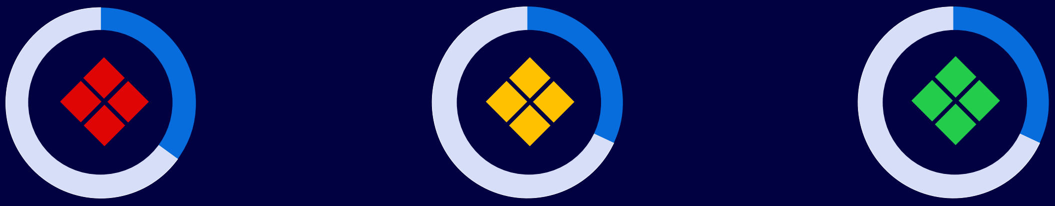
Leaders are taking a pragmatic approach

Within the biopharma and Life Sciences industries at large, new product innovation – like bringing new pharmaceuticals to market – is a process that can take 10 or more years to complete. Companies in this sector are making astronomical investments, from concept to marketing their new miracle cure.

A paper published by the **Journal of the American Medical Association (JAMA)** in 2020 estimated that **the median capitalized research and development cost per product was $1.1 billion**. This immense investment is predicated on the successful launch of new innovations to market, and should inform how those in the Life Sciences sector approach creating insider threat programs.

Most of the effective strategies for IP protection begin by taking the necessary time to identify and engage stakeholders who are invested in safeguarding the company's valuable assets. This includes the people, processes, and technologies critical to the business. However, it can be very difficult for cybersecurity leaders to prioritize data loss incidents and allocate the necessary resources.

Top 3 types of insider-driven data exposure, loss, leak, and theft events being investigated:



Critical/high-risk events **35%**

Moderate-risk events **32%**

Low-risk events **32%**

50% of data loss incidents are malicious, and our analysis of risk severity shows an estimated even split between low-, medium-, and high-risk incidents. The varying severity levels of incidents make it **challenging to prioritize detection and response**, leading to a lack of focus and efficiency for security teams, which adds a significant burden to teams' already limited resources in terms of time and personnel.

By empowering employees to act as the first line of defense against data breaches, organizations not only enhance their overall security posture but also **free up valuable time for specialized teams to focus on investigating and mitigating high-risk events**.

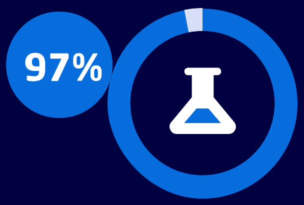
Integrating People and Processes for Robust IP Protection

The power of nuanced security training to harness the full potential of your workforce

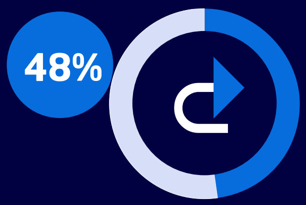
Organizations must uncover the subtle signs and patterns that may indicate threats from within, with a focus on the nuanced landscape of the health and Life Sciences sector. To do so effectively, cybersecurity leaders need to learn **how training can be used to increase engagement and foster an organizational culture that emphasizes security awareness and proactive efforts**. This will allow them to fortify defenses against internal threats to preserve the integrity of IP and trade secrets.

Particularly, the implementation of targeted and responsive data security training programs can be highly effective in mitigating lower-level risk events within organizations. In 2023, data security training was predominantly conducted weekly (34% in 2024, up from 30% in 2023). However, there has been a notable upward trend in organizations conducting training daily, rising from 11% in 2021 to 15% in 2023, and now reaching 27% in 2024. This significant increase in frequency could be attributed to the urgent necessity of addressing a persistently challenging problem that has not shown signs of improvement.

More Frequent Data Security Training Correlates with Fewer Incidents, but Life Sciences Respondents Seek Improvement



97% believe that their data security training programs **require further improvements**



48% believe their data security training requires **a complete overhaul**, a greater number than any other industry

Over all industries, **there is a clear correlation between training frequency and improvement of data security**, as organizations that conduct daily training experience fewer insider-driven data events per month, compared to those conducting training quarterly (with averages of 23 events versus 28 events, respectively). Despite this, almost all organizations in the life sciences sector (97%) believe that their data security training programs require further improvements – with 48% believing their programs require a complete overhaul, a greater number than any other industry.

These insights suggest that while regular data security training can enhance a company's ability to handle varying levels of insider-driven data incidents, its effectiveness is contingent upon the quality and comprehensiveness of the training program. This underscores the **critical importance of continually evaluating and improving data security training initiatives to effectively mitigate risks associated with insider threats**.

Organizations are thus increasingly seeking a comprehensive solution that not only swiftly detects and halts threats, but also streamlines response strategies within a single platform. This holistic approach advocates for automated training to handle low-risk data events without human intervention while simultaneously blocking unacceptable activities, presenting an optimal solution. The drive to consolidate data protection tools into fewer solutions has become a key objective, making products like Incydr a viable answer to reducing security product sprawl.

Best Practices to Protect Against Insider Threat

Data loss impacts time, money, and employees

Our 2024 Data Exposure Report shows that the Life Sciences sector is at the forefront of AI utilization, presenting new opportunities for cybersecurity teams to enable automated detection and response, as well as the resources to concentrate on strategic tasks. Protecting intellectual property (IP) remains paramount for Life Sciences companies, crucial for maintaining a competitive edge. However, tackling insider threat comprehensively demands a holistic approach to combat data loss effectively.

To aid security professionals, organizations must embrace technologies that go beyond mere detection and reactive responses. A robust solution should detect, prioritize, and respond to incidents while minimizing overall insider-driven risk. Equipping security professionals with the right tools and integrating comprehensive security programs not only simplifies their tasks but also fosters a proactive culture organization-wide, ready to address growing threats head-on. There are a few key factors that cybersecurity leaders can take into consideration when it comes to creating and implementing an insider threat solution:

Safeguard your trial data and maintain your competitive edge.

Given the lengthy process of new product development, preventing intellectual property leaks to competitors who might gain an early market entry is essential. Yet, ensuring visibility is paramount to safeguarding your data effectively.

Ensure swift and secure market entry.

Losing crucial information, whether through leaks or negligence, can significantly delay an already lengthy process. Safeguarding this value chain requires robust processes, strategic planning for data protection, and prompt response protocols when data is endangered.

Uphold customer trust and compliance standards.

Concentrating solely on regulatory compliance may obscure the ability of security and GRC teams to detect intellectual property losses, leading to mandatory disclosures and increased compliance risks.

Such disclosures can also negatively impact public perception and consumer confidence. Broaden your compliance perspective to encompass thorough visibility and insight into risky behaviors.

Methodology

Code42, now a Mimecast company, commissioned 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 headquartered 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. Of those participants, 144 were part of the Life Sciences/biotechnology sector.

This report sometimes references data from the now retired 2023 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. In addition, the scope has had some changes so caution has been taken when making comparisons to 2023 iterations. The main differences include:

Objective: The 2023 report focused on key drivers of data loss from insiders and challenges to building and running IRMs.