Annual Data Exposure Report 2022

code42

Key Findings

Today, data is a company's most valuable asset, leading many to invest in Insider Risk Management programs. Some industries, such as the Public Sector and Financial Services, are at the more mature end of the spectrum, leading the way in addressing Insider Risk. Recent trends around employee turnover and remote work have created unprecedented challenges for security teams to protect valuable data from leaving the company. There needs to be more investments around educating the Board, training employees, and increasing visibility to data movement.

Businesses are concerned that the Great Resignation is a catalyst for departing employees to unknowingly or intentionally expose, leak or exfiltrate IP

98%

of business leaders, cybersecurity leaders and cybersecurity practitioners have cybersecurity concerns with levels of turnover

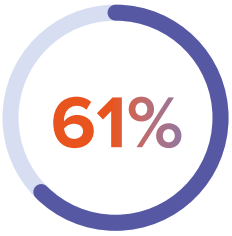
71%

Nearly three-fourths lack visibility over what and/or how much sensitive data departing employees take to other companies

71%

The same proportion are concerned about sensitive data saved on local machines/personal hard drives and/or personal cloud storage and services

Having an Insider Risk Management program is not enough as data suggests that most companies' programs are challenged with effectively protecting corporate data from Insider Risks

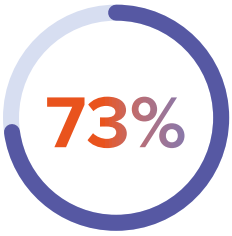


61%

say they have an Insider Risk Management program, while the average cybersecurity budget allocated to mitigating Insider Risk is 21%

96%

However, almost all experience challenges when it comes to protecting corporate data from Insider Risks



73%

report Insider Risk is a big problem within their company

91%

Lastly, 91% believe that their companies' Board requires more understanding of Insider Risk

Training must evolve to include education for employees on the right way to handle data

55%

Over half of respondents are concerned about employees becoming lax in their cybersecurity practices with a new hybrid work environment

96%

Almost all companies need to improve the data security training they provide employees, with around a third (32%) stating a complete overhaul is needed

Public sector and financial services industries are leading the way in Insider Risk Management

26% & 24%

Both industries are using around a quarter of their global cybersecurity budget to combat Insider Risk, on average

84% & 76%

Both have the highest percentage of companies with IRM programs in place

Pre-IPO companies are making Insider Risk Management a priority, given compliance requirements and the value of IP assets in IPO transactions

77%

Pre-IPO companies are most likely to have an IRM program

85%

Insider Risk is a Board-level priority for 85% of pre-IPO companies, with 82% indicating Insider Risk is discussed at every Board meeting

51%

Pre-IPO companies are much more likely (51%) to make Insider Risk Management a top priority, compared to those who had a major merger, acquisition or divestiture occur in the last 12 months (32%) or who have one planned in the next 12 months (26%)

Part 1

Introduction

As CISOs around the globe take stock of the cybersecurity landscape that has emerged as a result of the new hybrid-remote world, Insider Risk has emerged as a top priority - one that must be examined, understood and addressed from the top down.

Growing awareness has been driven in part by burgeoning recognition from top analyst firms that Insider Risk Management (IRM) is a significant cybersecurity challenge that must be prioritized. Gartner recently evolved the *User Entity Behavior Analytics (UEBA) category renaming it IRM*, after first *recognizing the new category* in December 2020. *Forrester* and *IDC* are also shining a spotlight on the importance of addressing Insider Risk.

Insider Risk is any user-driven data exposure event, either malicious, negligent or accidental in nature. Security leaders have recognized that managing Insider Risk is central to keeping their most important data - source code, product designs, customer information - from ending up in the wrong hands. The financial, reputational, privacy and compliance ramifications of sensitive data being exposed and leaked are significant. Even more significant is the risk of a company's intellectual property (IP) ending up in the hands of a competitor.

Unfortunately, there appears to be a four-way disconnect – between cybersecurity leaders, cybersecurity practitioners, business leaders and the Board – when it comes to addressing data exposure and exfiltration as a result of Insider Risk. Research suggests this disconnect exists due to a lack of visibility into the size and scope of the data exposure and exfiltration problem, coupled with a lack of understanding across the company on its likelihood and impact. Ownership of the Insider Risk problem also remains vaguely defined.

There are many factors at play for the rise in Insider Risk concerns, but four rise to the top based on the findings in this report. First, more and more employees are leaving their jobs than ever before. Coined the Great Resignation or Big Quit, we saw a record number of employees - 4.5 million – *leave their jobs in November 2021* alone. Second, there appears to be a culture of disconnect around the problem, which leads to uncertainty around ownership. Insider Risk is simply not being talked about enough from the top down or the bottom up. Third, companies need a better understanding of data movement. They don't just need more visibility, they need better, more contextual visibility to determine what data movement poses unacceptable risk to the business. Lastly, employees are simply unaware of the risk they pose to the company. Despite massive investments in time, resources and technology and training, employee security awareness remains a challenge.

Examining data from the *US Bureau of Labor Statistics* and previous DERs from *2020* and *2021*, reveals that there is a one in three (37%) chance your company loses IP when an employee quits. Comparing this to data from *Verizon DBIR 2020*, departing employees are the second highest cause of a successful data breach, only behind hackers (45%) and ahead of social engineering (22%), user error (22%), malware (17%) and user misuse (8%).

With a one in three chance that the company's Intellectual Property data is walking out the door with a former employee, are you willing to take those odds?

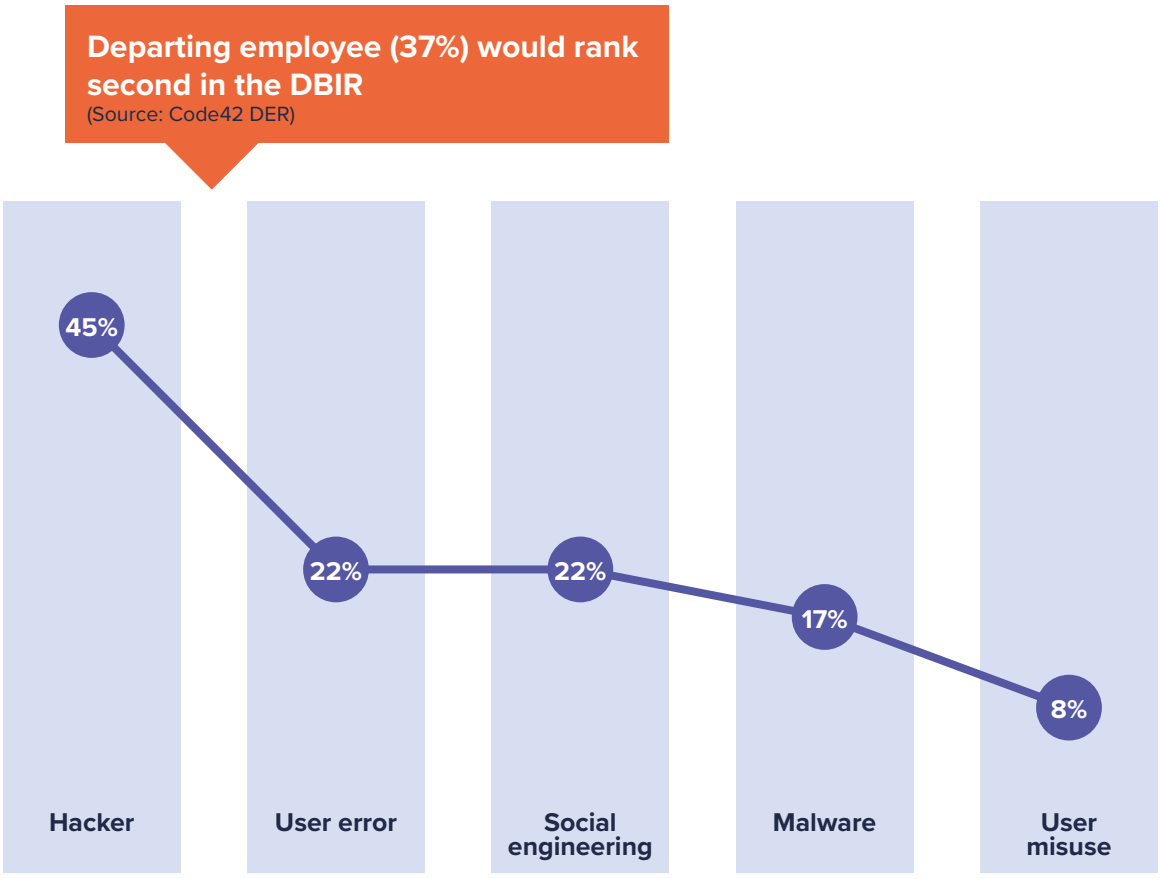


Figure 1: What tactics are utilized? (Actions) Source: Verizon DBIR 2020

Objective of the Annual Data Exposure Report 2022

In past Annual Data Exposure Reports, Code42 has researched who, what, when, where, how and why employees expose and/or exfiltrate data. In the 2022 edition, we wanted to understand the impact of data exposure and exfiltration and why companies are challenged to prioritize IRM even though it has become clear over the years that Insider Risk is a persistent problem for cybersecurity teams to effectively manage.

To explore this, we surveyed 700 respondents – senior business leaders, senior cybersecurity leaders and cybersecurity practitioners – from US companies with 500 or more employees from a range of public and private sectors.

Part 2

The Great Resignation

Companies lack visibility into what types of data are leaving and how

With a record *4.5 million people quitting their jobs in November 2021*, the Great Resignation rages on and it's no wonder nearly all (98%) respondents have cybersecurity concerns about their employees leaving the company. Nearly three-fourths (71%) are concerned about lack of visibility over what and/or how much sensitive data departing employees take to other companies. The same proportion (71%) are concerned about sensitive data saved on local machines/personal hard drives and/or personal cloud storage and services. These concerns are not surprising, given real-world examples of employees *taking data with them to competitors*, or even worse, leveraging it to *hold their former employers for ransom.*

Looking specifically at the three groups surveyed, the differing concerns of business leaders, cybersecurity leaders and cybersecurity practitioners stand out. Business leaders are most concerned about lack of visibility into what types of data are leaving (49%) while cybersecurity practitioners are most likely to be concerned about data being saved on local machines or personal hard drives (52%). This highlights how business leaders are more concerned about the *content* of the data that is exposed, while practitioners are predictably more concerned about *how* data is being exposed. This is not surprising given the nature of each groups' roles.

98%

Nearly all respondents have **cybersecurity concern(s)** with their employees leaving their company during the **Great Resignation**

71%

are concerned about **lack of visibility** over what and/or how much **sensitive data departing employees** take to **other companies**

71%

are concerned about **sensitive data** saved on **local machines/personal hard drives** and/or **personal cloud storage and services**

Cybersecurity concerns regarding employees leaving the company

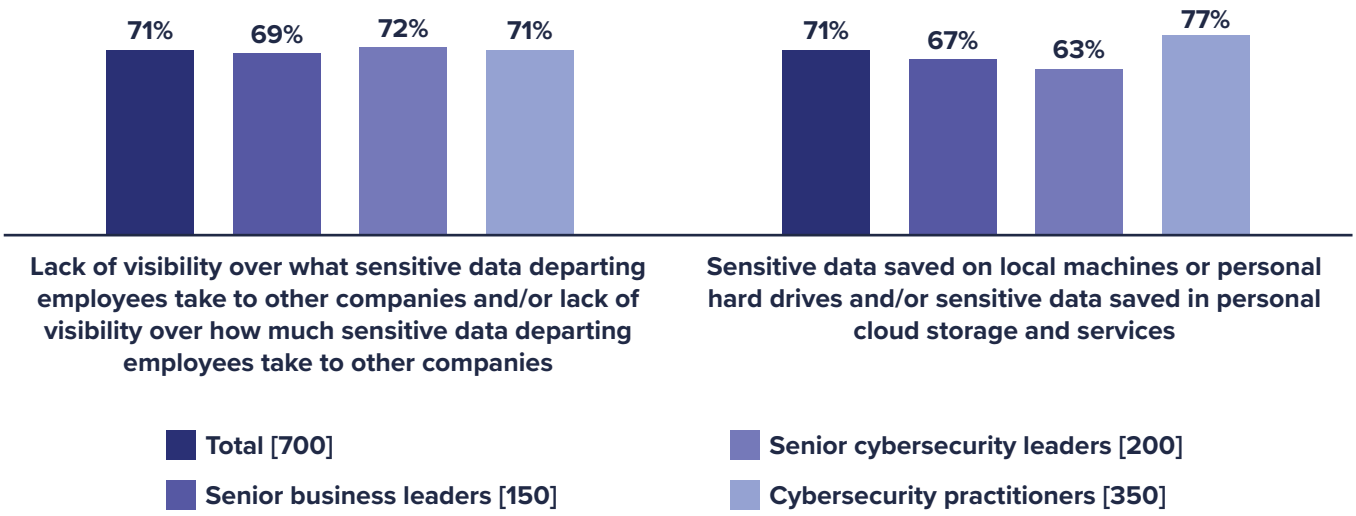


Figure 2: In April 2021, a record 4 million people quit their jobs, starting what is called the "Great Resignation" period. What cybersecurity concerns do you have regarding employees leaving your company during the Great Resignation? [Base sizes in chart], split by respondent type, omitting some answer options

The discrepancy between the percentage of cybersecurity practitioners (77%) versus the percentage of cybersecurity leaders (63%) that are concerned about sensitive data saved on local machines, personal hard drives or personal cloud storage is also significant and likely indicates how much data exposure practitioners are witnessing via these vectors, while security leaders at some companies are potentially not engaged enough to grasp the full scope of the problem.

The pandemic has brought about a huge surge in remote working which has certainly contributed to greater Insider Risk - almost all respondents (97%) report having cybersecurity concerns as a result. However, it is far fewer (43%) who report that improving technologies for a remote/hybrid workforce is a top two priority for their company, suggesting a gap between concern and prioritization for the security of a remote workforce.

Companies' biggest cybersecurity concerns following the pandemic

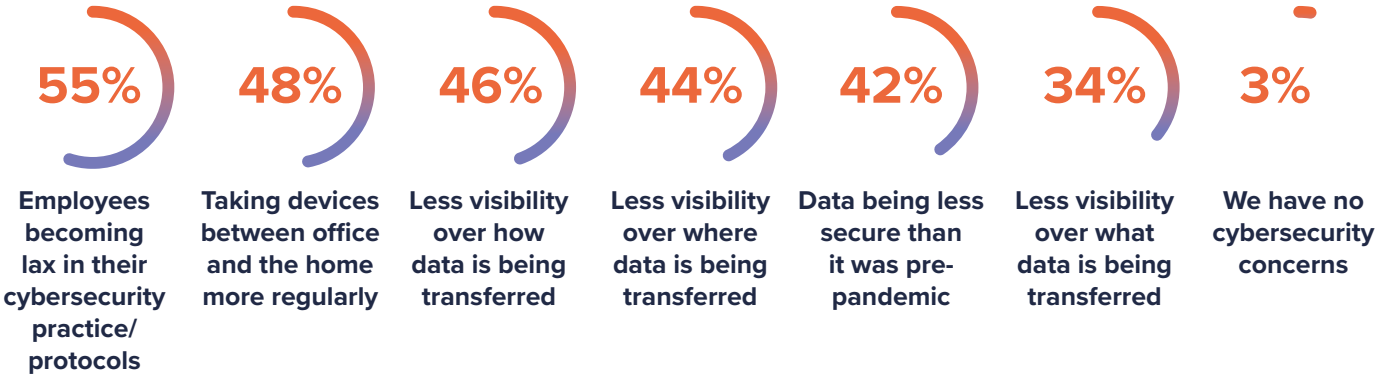


Figure 3: What are your company's biggest cybersecurity concerns with a return to the office or a new hybrid workforce, as a result of the COVID-19 pandemic? [700] omitting some answer options

Part 3

Culture of Disconnect

Practitioners Left in The Dark while Cybersecurity Leaders Fight for a Voice in Business Decisions

Cybersecurity practitioners want a louder voice when it comes to setting the cybersecurity posture and priorities of their company, as they should – they're the ones dealing minute-by-minute with the risks their company's face. Today, practitioners report a lack of transparency – and consultation – from cybersecurity leaders around the decisions that are made. Unfortunately, cybersecurity leaders appear stuck between a rock and a hard place – spending more time consulting their teams for on-the-ground insight or addressing compliance mandates and Board demands. It leaves one very real question unanswered: how do you measure improvement and success?

58%

Nearly three in five cybersecurity practitioners report that **cybersecurity leaders don't communicate the company vision** to the rest of the cybersecurity team

57%

of practitioners report that they aren't **consulted about decisions that are made** based on companies' cybersecurity strategies

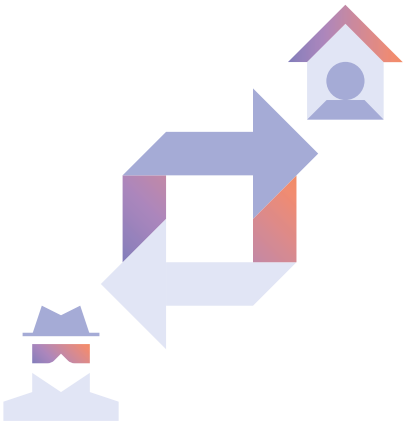
Policies continue to hamstring teams

Almost all (96%) companies experience challenges when it comes to protecting corporate data from Insider Risks. When looking at these challenges, it's cybersecurity practitioners who are more directly affected. For example, half (50%) of these respondents report difficulties keeping policies up to date at the rate the business needs, compared to cybersecurity leaders (35%) and business leaders (38%). Policies that impede on employee productivity and collaboration is a challenge reported more heavily by practitioners (45%) versus cybersecurity leaders (38%) and business leaders (38%). With practitioners being more likely to use these policies, they are more likely to be suffering from using outdated tools and therefore understand the importance of a modern approach to security and collaboration, something that leaders are further removed from. This data highlights the disconnect between cybersecurity practitioners, security leaders, business leaders and Boards.

Cybersecurity professionals are on the front lines confronting Insider Risk on a daily basis and have a more complete understanding of its scope and impact, but are rarely consulted on how to address the problem.

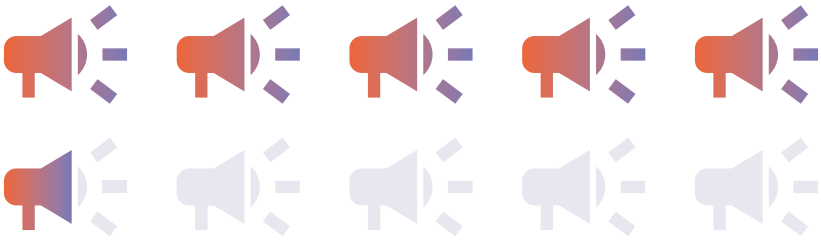
96% of companies experience **challenges** when it comes to **protecting corporate data** from Insider Risks

Bottom to top, there is a lack of transparency around the Insider Risk problem and it's creating churn and frustration for the cybersecurity practitioners who see firsthand the size and scope of the Insider Risk problem, but cannot measure it. As our research shows, 98% of companies are concerned about Insider Risk indicating a vast majority have a data exposure problem. When it comes to measuring Insider Risk, companies should start with establishing a data exposure baseline. Cybersecurity practitioners should make sure they have certain metrics at their fingertips, including the percentage of all corporate data residing in untrusted locations by file category, the number of data exposure events by risk severity, the number of high severity data exposure events contained and the percentage improvement in data exposure events over time. If cybersecurity practitioners cannot measure Insider Risk, then cybersecurity leaders cannot quantify Insider Risk. If cybersecurity leaders cannot quantify the risk, then business leaders will never understand the impact, and if business impact is not understood, Boards will never prioritize the problem.



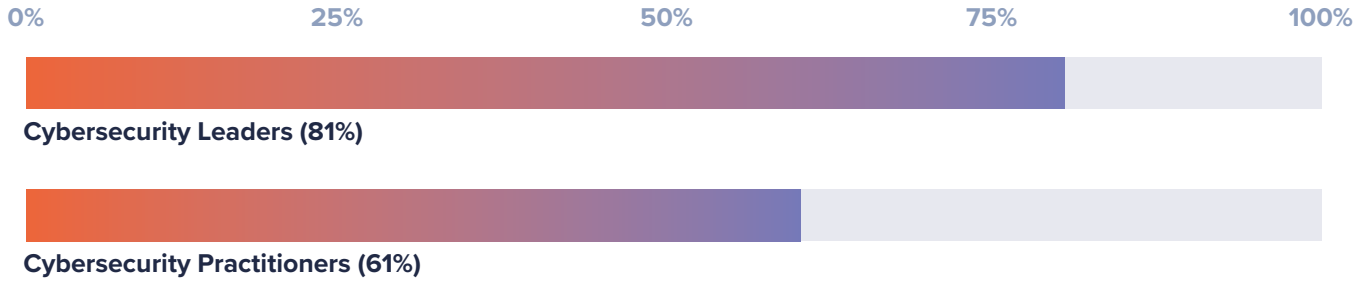
This vicious cycle has been going on for years only to be amplified by the Great Resignation, remote and hybrid work and a barrage of IP theft cases spotlighted in the news media. Managing Insider Risk starts with practitioners having the means to measure it and communicate up the chain.

56% of cybersecurity leaders and practitioners agree that they **don't feel** like they have a **strong voice in business decisions** made by the leadership team



There is a disconnect from the perspectives of cybersecurity practitioners and leaders when reporting how frequently Insider Risk is a topic of discussion at Board meetings. The vast majority (81%) of cybersecurity leaders – 20% more than practitioners (61%) – report that Insider Risks are discussed at every meeting. Are cybersecurity practitioners receiving effective information from Boards regarding Insider Risk? This data suggests that Boards believe they are having the right conversations to address Insider Risk, but are perhaps still not grasping the full scope of the problem.

Insider Risk is a topic of discussion at every Board meeting



In order to improve the issues with transparent communication around the impact of Insider Risk, all parts of the business need to become better at collaborating. This starts by communicating the size and scope of Insider Risk and what it means to executive and Board-level business objectives. However, almost all (91%) respondents believe that their companies' Board requires more understanding of Insider Risk, so creating appropriate objectives and communicating them to the business likely is not happening, at least not effectively.

The findings show that Boards are strongly influencing cybersecurity leaders' ability to make decisions, but who's influencing the Board? A barrier to increasing Board level understanding of Insider Risk is who they listen to. The data governance and compliance team doesn't place enough attention on Insider Risk (70%), yet cybersecurity respondents (45%) feel that the Board listens more to regulations than they do to them.

believe that their companies' **Board requires more understanding of Insider Risk**

Part 4

Budget & Programs

Security needs Insider Risk metrics in order to secure budget to build more effective programs

21%

of current **cybersecurity budgets** go to **Insider Risk Management,** on average

65%

believe **Insider Risk Management budgets will increase** this coming year

Only 21% of companies' cybersecurity budgets are currently dedicated to mitigating Insider Risk, on average. In 2021* , 54% of cybersecurity leaders spent less than 20% of their budgets on Insider Risk. However, acceptance of the need to increase the budget is increasing, with 73% of respondents stating that their companies' budget for protecting against Insider Risk is insufficient, up from 66% of cybersecurity leaders who cited this in last year's report* . There is positive momentum, however – companies are recognizing that Insider Risk is a pressing concern and the impacts need to be avoided. Nearly two-thirds (65%) believe they will be successful in securing a larger budget for Insider Risk Management in the coming year.

The need for an Insider Risk Management (IRM) program is clear, with 61% of companies currently using one and 36% planning to implement one in the future. Respondents from financial services (76%) and the public sector (84%) are leading the way and most likely to report that their company has an IRM program, while those in media, leisure and entertainment (44%) and business and professional services (47%) are lagging behind and the least likely to.

61%

of companies surveyed have an IRM program

* Figures were lifted from the 2021 DER. Please see methodology for more information

98%

have **fears regarding Insider Risk** events in their company

80%

Eight in ten report that **reputation** has/would be impacted because of an Insider Risk event involving loss or theft of sensitive information

Concerningly, 98% of respondents have fears regarding Insider Risk events in their company, with reputational damage, loss of IP/customer data and revenue loss being the three most likely fears.

These fears are at risk of becoming reality as eight in ten (80%) report that reputation has/would be impacted because of an Insider Risk event involving loss or theft of sensitive information, with this being more likely for those without an IRM program (84%). These impacts should serve as significant motivators for those without an IRM program to implement one.

However, while 61% of companies say they have an Insider Risk Management program, 73% of respondents report Insider Risk is still a big problem within their company. Surprisingly though, the majority (63%) of surveyed companies do not measure the success of Insider Risk detection. This disconnect begs the question - have companies with an IRM program implemented one that is truly effective? Companies that have a program are likely to be more risk-aware because they invested in one in the first place, but these results suggest challenges persist. It could be that, for those companies, taking the first steps in implementing an IRM program has highlighted just how much data exposure exists within their company, crystalizing how much more work needs to be done. This is likely an important turning point for companies, to realize that an effective Insider Risk Management program balances and measures each element of people, process and technology.

73%

report **Insider Risk is a big problem** within their company

63%

of companies **do not measure the success of Insider Risk detection**

Part 5
Training

Insiders need better training, with content more relevant to their unique workforce

55%

Over half are **concerned** about **employees becoming lax in their cybersecurity practices/protocols**

70%

of those in the public sector are **concerned** about **employees becoming lax in their cybersecurity practices/protocols**

Nearly two years into the pandemic, companies are still adapting to new ways of working, with some choosing to go permanently fully remote and others returning to the office in starts and stops. For the majority, managing a hybrid workforce will be a near-term reality. This presents a number of cybersecurity challenges, with over half (55%) of surveyed respondents sharing concerns about employees becoming lax in their cybersecurity practices/protocols, a feeling that is particularly strong for those in the public sector (70%).

This data demonstrates the critical need for security education and awareness training, particularly during this new era of hybrid work. Companies can mitigate risk by changing user behavior through training, creating a more risk-aware workforce. Frequency and quality of training are two of the most important variables. It is most common for companies to conduct security training on a monthly basis. For around a third (32%) of companies this is the case, followed by weekly (22%), quarterly (20%), daily (11%) and annually (9%).

Surprisingly, after parsing the data in search of correlations, the data shows that companies conducting training more frequently (daily or weekly) are actually more likely to find it difficult to detect Insider Risk and see Insider Risk as a big problem for their company, compared to those conducting it monthly or quarterly (see figure 4). This leads to a question as to whether companies that report providing training more frequently are offering training that is truly effective. It can be deduced from this data that companies providing training on a monthly or quarterly basis are providing more quality, relevant training that leads to fewer challenges with Insider Risk within their company.

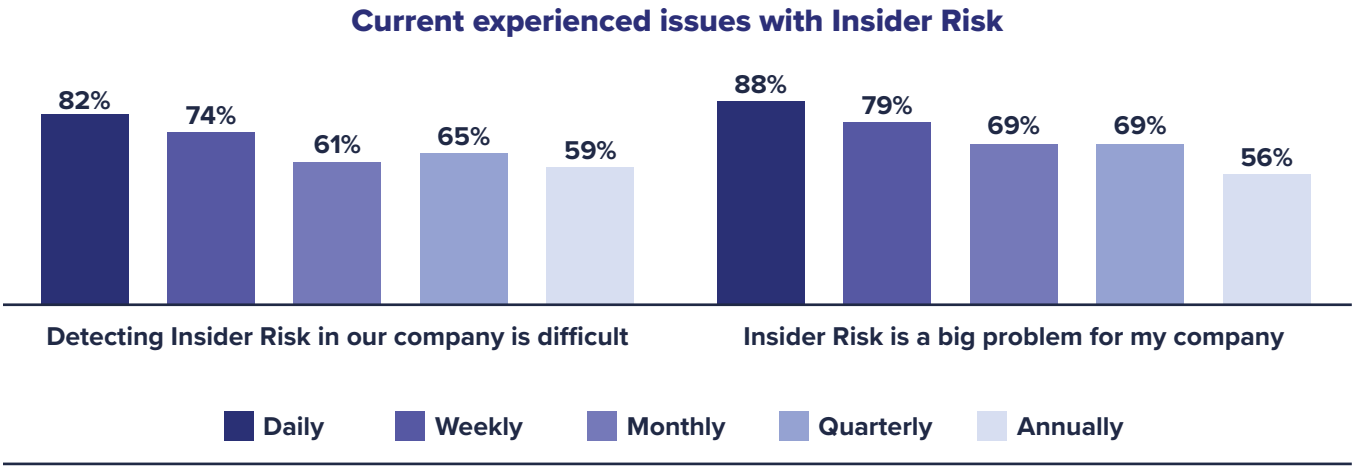


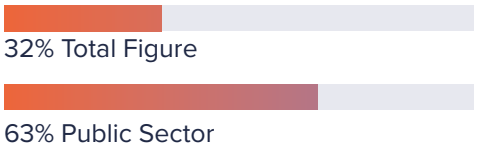
Figure 4: To what extent do you agree or disagree with the following statements? Strongly agree or somewhat agree [700] omitting some answer options, split by frequency of data security training

Almost all (96%) companies need to improve the data security training they give to employees. In fact, around a third (32%) say a complete overhaul is needed, with those in the public sector being the most likely industry to say this (63%). Companies have a lot of work to do to improve the training they offer to their employees to ensure the content is relevant for each unique workforce.

96%

of companies need to **improve** their **data security training**

A **complete overhaul** is needed to data security training



With these results in mind, there are two areas that companies should focus on when conducting training – the frequency and the quality. Training employees should be both proactive and responsive. Proactively, in order to change employee behavior, companies should provide both long- and short-form training modules to instruct and remind users of best behaviors. Additionally, companies should respond with a micro-learning approach using bite-sized videos designed to address highly specific situations. The security team needs to take a page from marketing, focusing on repetitive messages delivered to the right people at the right time.

Part 6

Industry breakout

When reviewing responses by industry, public sector and financial services companies are leading the way in Insider Risk Management and protecting valuable data, based on the percentage of their global cybersecurity budget dedicated to mitigating the problem. Both industries are using around a quarter (26% and 24%) of their global cybersecurity budget to combat Insider Risk.

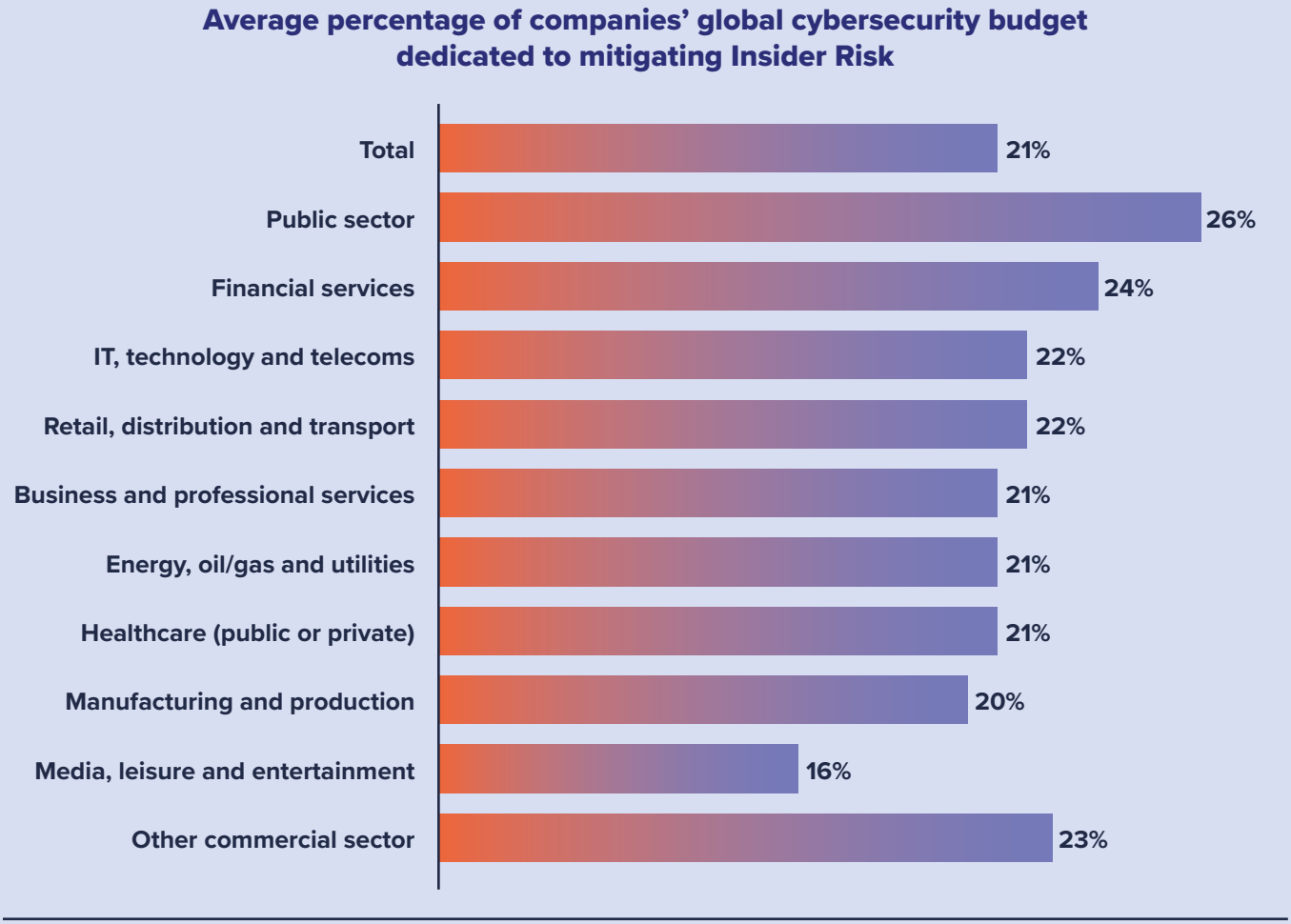


Figure 5: What percentage of your company's global cybersecurity budget is dedicated to mitigating Insider Risk? [700], showing average scores, split by industry

It's both the public sector (84%) and financial services industry (76%) that have the highest percentage of companies with an IRM program in place, which is perhaps not surprising given the potential historical impacts of an insider breach in these two sectors. Media, leisure and entertainment companies have the smallest average budget allocated to mitigating Insider Risk (16%), which could explain why they are the least likely to have an IRM program (44%). This lackluster approach is concerning, particularly when considering the challenges the media industry is facing at the moment. Policies impeding on employee productivity (47%), difficulties keeping policies up to date at the rate of business needs (45%) and solutions failing to detect relevant data and files, i.e., false negatives (44%) are just a few of the issues faced in relation to Insider Risk for media.

Figure 6: Does your company have an Insider Risk Management progam? [700], showing proportion who said “Yes” split by industry

Furthermore, as a result of the COVID-19 pandemic, it’s companies within the public sector that are most likely to be or are planning to add new cybersecurity technologies for better monitoring of file movements, with almost six in ten (58%) reporting so. Of course, with this comes a greater need to set aside budget to mitigate Insider Risk. For financial services, greater emphasis is put on more adoption, training and enforcement around collaboration tools as reported by more than half (57%).

With 98% of surveyed companies in the financial industry reporting having fears regarding Insider Risk, it’s critical that such events are mitigated. But it is not just financial services that have these fears – they’re present across all industries. Those in healthcare (public or private) are the most likely to fear reputational damage (72%), which makes sense given the sensitive nature of the data they collect and store. Loss of IP/customer data is feared most for those in retail distribution and transport (59%), as is revenue loss (54%). It is those in the energy, oil/gas and utilities sector that are the most likely to fear their ability to hire and retain employees (57%) as a result of Insider Risk events. While fears are present across all industries, the specific fears that are felt differ by how Insider Risk events impact industries.

Part 7

Company maturity breakout

Respondents were asked to identify the current stage of their company's evolution, choosing between:

IPO planned for the next 12-18 months	**Major Merger, Acquisition or Divestiture planned for the next 12 months**	**Major Merger, Acquisition or Divestiture occurred in the last 12 months**	**Major Restructuring (organizational change with potential layoffs) planned for the next 12 months**	**Major Restructuring (organizational change with potential layoffs) occurred in the last 12 months**	**Not aware of any major changes in the next 12 months**

Companies, regardless of their maturity, are likely to list improving cybersecurity against external threats as among one of their top two information security priorities. Companies of various maturity levels diverge, however, when it comes to Insider Risk. Companies with an IPO planned for the next 12-18 months are prioritizing managing Insider Risk in a number of ways. Pre-IPO companies are much more likely (51%) to make Insider Risk Management a top priority, compared to those who had a major merger, acquisition or divestiture occur in the last 12 months (32%) or who have one planned in the next 12 months (26%).

It is not surprising that pre-IPO companies are making Insider Risk Management a priority, given that IP is a valuable asset during IPO transactions. Pre-IPO companies are also likely driven by the compliance requirements around security controls that they must adhere to after filing to go public. Pre-IPO companies are most likely to have an IRM program (77%). Even more, Insider Risk is a Board-level priority for 85% of pre-IPO companies, with 82% indicating Insider Risk is discussed at every Board meeting.

Pre-IPO companies are **most likely** to have an IRM program

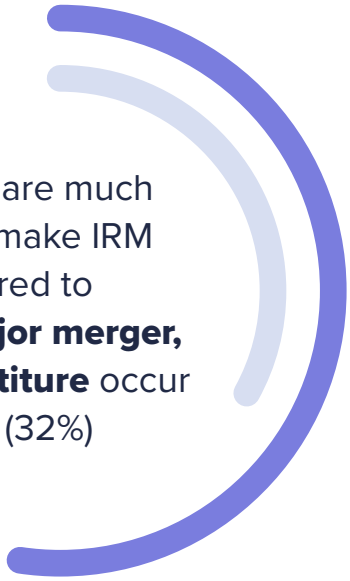
Total Figure 61%

Pre-IPO Companies 77%

85%

Insider Risk is a **Board-level priority** for 85% of pre-IPO companies

Pre-IPO companies are much **more likely** (51%) to make IRM a top priority, compared to those who had a **major merger, acquisition or divestiture** occur in the last 12 months (32%)



"We had 90 to 120 days before going public to have a solution and a really tight story about our insider threat program,"

says Mario Duarte, ***Snowflake's*** VP of Security.

Regardless of maturity, reputational damage as a result of Insider Risk events is the number one concern across all companies. But there are some differences in the proportion who have other fears. One surprising finding is that loss of IP/customer data is more likely to be a fear for companies that had a major merger, acquisition or divestiture in the last 12 months (51%) than it is for those that have one planned in the next 12 months (35%), perhaps due to employees departing post-merger. This could signal a level of naivety around IP pre-merger and that going through a major transition - and potentially making some mistakes along the way - makes companies realize just how important it is to effectively protect IP.

Part 8
Conclusion

Companies need to start challenging their approach to Insider Risk, with the results of this research suggesting three main areas to focus on:

Trust and transparency

We're seeing a disconnect at every level of the business, particularly among business leaders and the cybersecurity team. Leaders need to work with the cybersecurity team to tackle Insider Risks and produce a well-thought-out policy on data handling that can be delivered to their employees. Cybersecurity practitioners need to be transparent with cybersecurity leaders on the size and scope of the problem. Cybersecurity leaders need to trust practitioners have a good grasp on the extent of the data exposure and Insider Risk problem. The missing component around trust and transparency is metrics; for example, the percentage of all corporate data residing in untrusted locations by file category, the number of data exposure events by risk severity, the number of high severity data exposure events contained and the percentage improvement in data exposure events over time. Without the right Insider Risk metrics, transparency and trust is not possible be it decisions made bottom to top, or top to bottom.

Training

Alongside reducing the disconnect across the company, employees need to be educated on the business impact of their actions, and this needs to be done through collaborative training that is in line with corporate policy and culture. At present, very few companies are satisfied with the training that is provided to their employees on Insider Risk so business leaders, cybersecurity leaders and practitioners could all benefit from investing in an employee training program dedicated to reducing Insider Risk.

Insider Risk Management (IRM) program

Many companies are seeing the benefits of an IRM program or recognize the need to have one. While being consistently transparent and delivering robust training programs are key to the success of mitigating Insider Risk, there is always going to be exposure to company data and thus business impact and risk from the actions of insiders. Companies need to take a good look at their IRM program or lack thereof. Starting with people and process requirements rooted in understanding the likelihood and business impact of Insider Risk events. Technology plays a major role in enabling business leaders, cybersecurity leaders and Boards to understand their Insider Risk exposure and impact. Focusing on exposure and potential impact enables security teams to establish the right metrics to measure Insider Risk posture and maturity overtime, report that to the business leaders and the Board, and everybody wins.

Part 9
Methodology

Code42 commissioned independent market research agency Vanson Bourne to conduct the Data Exposure Research. The 2022 study surveyed 700 respondents (150 senior business leaders, 200 senior cybersecurity leaders, 350 cybersecurity practitioners) from companies in the US in September and October 2021. These companies had 500 or more employees and were from a range of public and private sectors, including business and professional services, financial services, IT and telecoms, and media, leisure and entertainment, 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.

Vanson Bourne conducted the 2022 DER. Any figures from previous DERs have been lifted directly from the reports that Vanson Bourne did not conduct.

Code42 has in the past worked with various research firms and previously published Annual Data Exposure Reports in *2018*, *2019*, *2020* and *2021 volume I* and *2021 volume II*.

About Code42:
Code42 is the Insider Risk Management leader. Native to the cloud, the Code42® Incydr™ solution rapidly detects data loss, leak and theft as well as speeds incident response – all without lengthy deployments, complex policy management or blocking employee productivity. The Code42® Instructor™solution helps enterprises rapidly mature their Insider Risk Management programs by incorporating holistic, hyper-relevant Insider Risk education for end-users to reduce risk events due to accidental and negligent behavior.

With Code42, security professionals can protect corporate data and reduce insider threats while fostering an open and collaborative culture for employees. Backed by security best practices and control requirements, the Code42 Incydr solution is FedRAMP authorized and can be configured for GDPR, HIPAA, PCI and other regulatory frameworks.

More than 50,000 organizations worldwide, including the most recognized brands in business and education, rely on Code42 to safeguard their ideas. Founded in 2001, the company is headquartered in Minneapolis, Minnesota, and is backed by Accel Partners, JMI Equity, NewView Capital and Split Rock Partners. Code42 was recognized by Inc. magazine as one of America's best workplaces in 2020 and 2021. For more information, visit code42.com or join the conversation on our ***blog***, ***LinkedIn***, ***Twitter*** and ***YouTube***.

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.***