DATA EXPOSURE REPORT 2021

CODE42

Ponemon INSTITUTE

Code42 Data Exposure Report

COVID-19 Creates Perfect Storm for Insider Risk Growth, Organizations Unprepared to Protect Data

Research Conducted by
Ponemon Institute for Code42

Published December 2020

CODE42

Part 1
Introduction

Insider Risk is a broad data protection issue that affects every organization. It is an outcome of employees getting their work done – accessing, creating and sharing files and data – in today's collaboration culture. It's unavoidable. Left unchecked, though, Insider Risks to data could threaten the future of the digital enterprise.

The purpose of *The Code42 2021 Data Exposure Report on Insider Risk* is to gain a better understanding of the many dimensions – from technology, process and budget to market conditions and internal perceptions – that impact organizations' security posture around Insider Risk to data. To craft this report, Code42 worked with Ponemon Institute in October of 2020 on a survey of US-based IT security leaders and business decision makers. This report represents a summary of those survey findings. Over the coming months, Code42 will release several subsequent reports, each diving deeper and revealing insights into specific topics outlined here.

Executive Summary

The study found that both business and security leaders are allowing massive Insider Risk problems to fester in the aftermath of the significant shift to remote work in the past year. In this report, we examine a number of factors, which we believe are leading to this growing threat.

Importantly, COVID-19 was a force accelerator and perfect storm during 2020 for insiders to put data at risk.

85%

KEY FINDING:
Employees are 85% more likely today to leak files than they were pre-COVID.

Organizations are faced with multiple challenges when it comes to building and running Insider Risk programs.

54%

KEY FINDING:
More than half (54%) of organizations don't have an Insider Risk Response Plan and 40% don't assess how effectively their technologies mitigate insider threats.

Security teams are operating in maintenance mode with outdated tools, which aren't adapted to the collaboration tech we use in our daily work – and that is leaving organizations exposed as they look to the future.

59%

KEY FINDING:
59% of IT security leaders expect Insider Risks to increase in the next two years.

When it comes to **Insider Risk**, is your business prepared for what's to come?

Part 2

COVID-19 has exacerbated an already growing threat.

Prior to the pandemic, cloud-based collaboration technologies and workforce turnover had become major drivers of data exfiltration as Insider Risk programs were failing to keep pace with today's digital workplace. Insider Risk is certainly not a new threat vector, but with our new work-from-home normal, and rising employee burnout rates, companies just can't keep up.

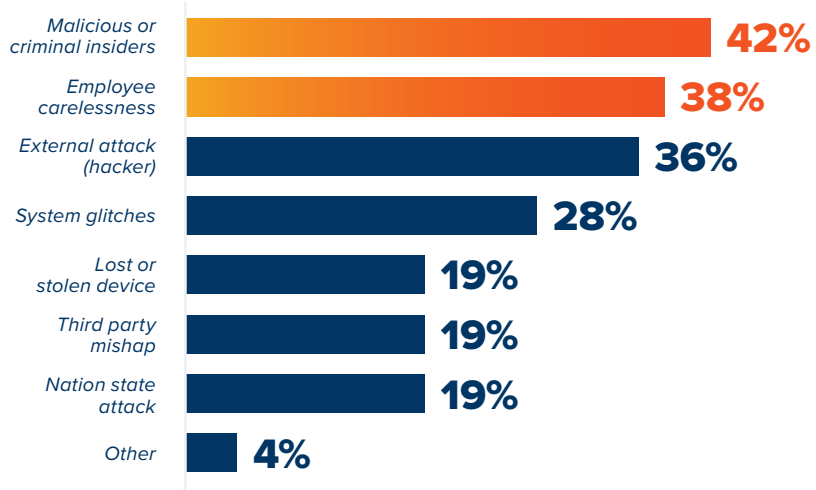
In the past year, **76% of IT security leaders say their organization has experienced one or more data breaches involving the loss or theft of sensitive information** contained in documents or files.

They also reported that the two most common causes of these data breaches were malicious or criminal insiders and employee carelessness followed by external attacks and system glitches, to name a few.

of organizations have experienced a data breach involving the loss or theft of sensitive information

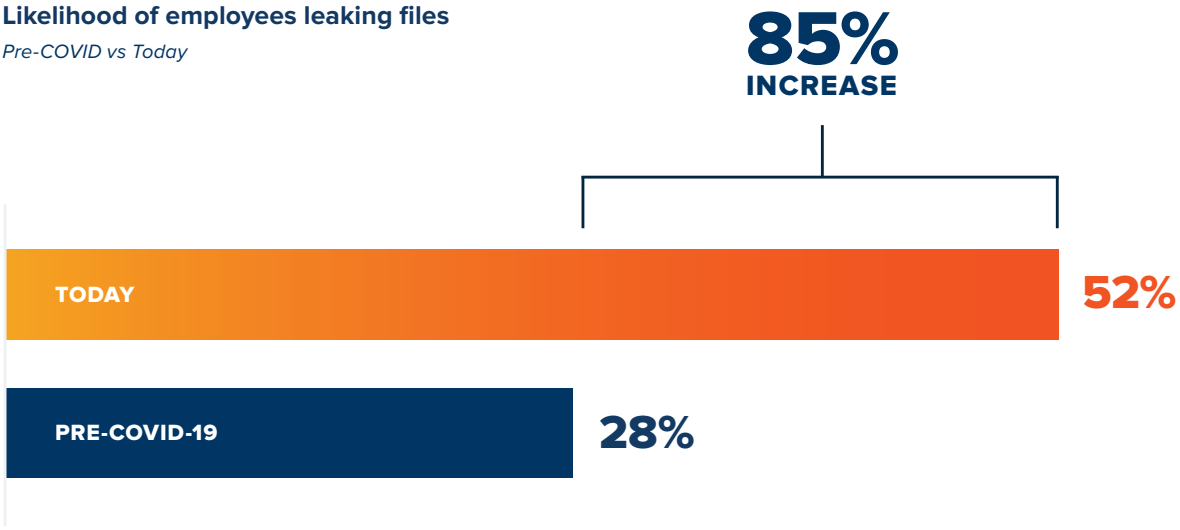
Most common causes of a data breach

According to IT security leaders



Likelihood of employees leaking files

Pre-COVID vs Today



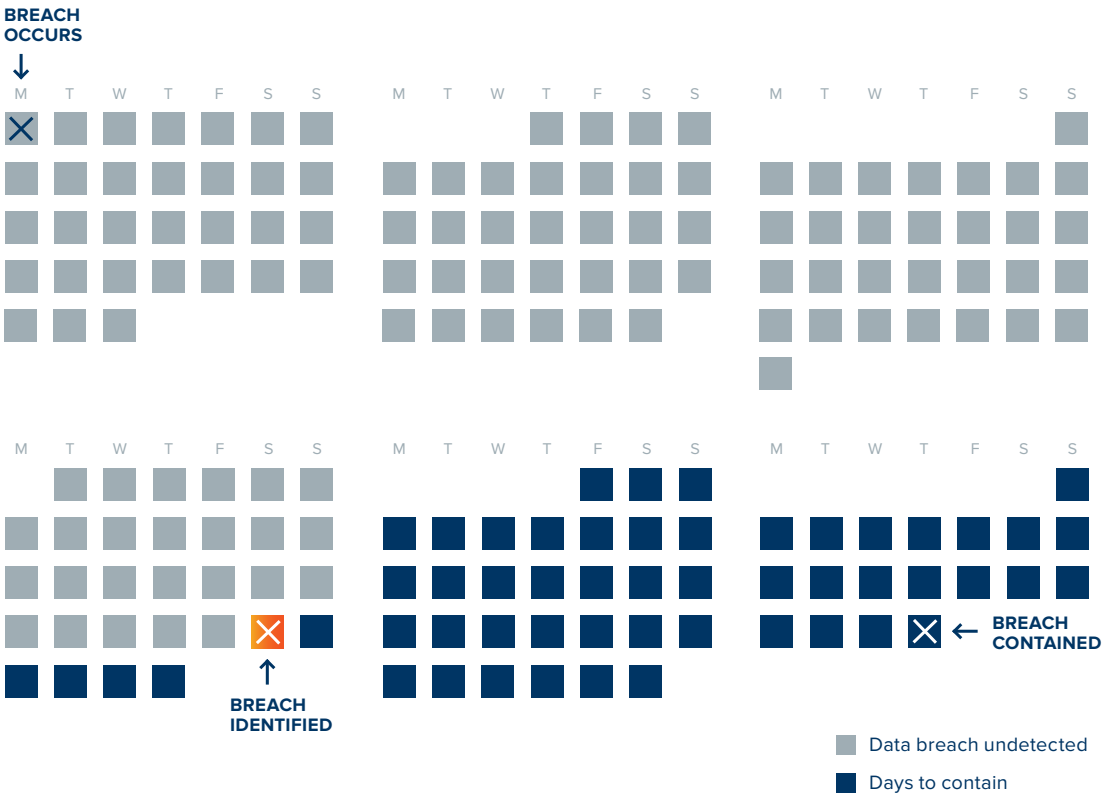
A remote, unsupervised, collaborating, off-network workforce creates a perfect storm for data leaks from insiders. **Since COVID-19**, **61% of IT security leaders said their remote workforce was the cause of a data breach.** They also reported that since the start of the pandemic, their employees have been **85% more likely to leak files than they were pre-COVID** (28% pre-COVID to 52% today).

According to IT security leaders, remote workforces pose a greater risk to data because home networks are less secure (71%) and employees do not follow security protocols as closely as they do when they're in the office (62%).

Part 3

Organizations face challenges on all fronts when dealing with Insider Risk.

According to IT security leaders, it takes an average of 118 days to identify a data breach and 55 days to contain one – a nearly six month process. Why is that?



Attitudes about ownership of work products have shifted over time.

More than **three-quarters (80%) of business decision makers believe they are entitled to or should own their work product.** In 2019, 71% of business decision makers felt entitled to their work, up slightly over 2018 when 65% of leaders felt they do or should own their work product.

Business decision makers who believe they are entitled to or should own their work product

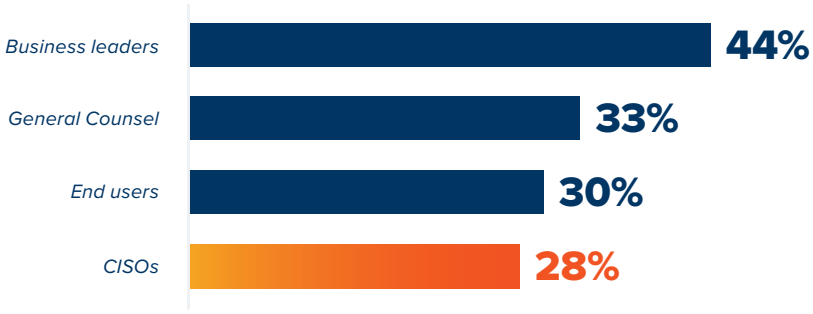
** Historical figures sourced from research provided by Sapio Research for Code42 2018 Data Exposure Report and Code42 2019 Data Exposure Report.*

If everyone owns security, then no one owns security.

It is not clear who has ultimate authority and responsibility for controlling and mitigating the insider threat challenge. IT Security leaders put line of **business leaders (44%), General Counsel (33%)** and **end users (30%)** ahead of even **CISOs (28%).**

Survey respondents identified the primary challenges to mitigating insider threat. They say it comes down to a lack of collaboration between IT security and lines of business (61%); a lack of leadership (51%); not being a priority (48%); and a lack in-house expertise (43%).

IT security leader responses to the question, "*who has ultimate authority and responsibility for controlling and mitigating the insider threat challenge*?"



Security is more accountable than they are admitting.

of organizations have an insider risk response plan

Insider Risk response processes are broken.

The C-suite and board of directors are under-informed about their organization's insider threat posture on a near-term regular basis. IT security leaders say in 70% of organizations, the C-suite and board of directors are **briefed on insider threats annually, only when requested, on an ad-hoc basis or not at all.**

Less than half of organizations, a mere 46%, have an Insider Risk response plan (IRRP). Of those with an IRRP, 71% apply it inconsistently or on an ad hoc basis.

of respondents do not regularly assess how effectively their technologies mitigate insider threats

Security tools for Insider Risk are not adapted to the way we work.

Nearly three-quarters (71%) of security teams lack complete visibility to sensitive data movement, according to IT security leaders.

The vast majority (91%) of security teams do NOT have purpose-built technology to document insider threat cases.

Forty percent (40%) of survey respondents say they **do not regularly or ever assess how effectively their technologies mitigate insider threats**.

2 IN 3

IT security leaders believe their budget for Insider Risk is insufficient

Budget issues prevail.

Two-thirds (66%) of IT security leaders believe their budget for Insider Risk is insufficient, and 54% of IT security leaders spend less than 20% of their budgets on Insider Risk.

Part 4

With Insider Risks predicted to increase, security teams need to mature their capabilities – and DLP is not the answer

Fifty-nine percent (59%) of IT security leaders say Insider Risk will increase or increase significantly in the next two years.

Employees are being disrupted while trying to do legitimate work. Over half (51%) of IT security leaders receive daily or weekly complaints about mistakenly blocking legitimate employee file activity. That means security teams are spending time managing policy exceptions on a daily or weekly basis. This validates that technologies that block file sharing have a negative impact on productivity for both employees and security teams.

of security teams lack historical context into user behavior

2 IN 3

security professionals don't know which Insider Risks to prioritize

Files moving from endpoint to cloud services and applications, whether employees are on or off the network, are the biggest Insider Risk blindspots for security teams.

More than half (53%) of security teams are blind to users moving files to untrusted domains. **And 56% of security teams lack historical context into user behavior.** In other words, security teams have no idea when an employee may become an Insider Risk.

Technology continues to fall short when it comes to risk prioritization. **Nearly two-thirds (63%) of IT security leaders don't know which Insider Risks to prioritize.**

Part 5
Conclusion

Insider Risk is a major wave that will continue to hit organizations in 2021, and so far, too few organizations have a life vest. To keep Insider Risk in check and preserve your digital enterprise:

Embrace, then secure the collaboration culture.

The pandemic proved a few things to businesses. It showed that employees today are more likely to leak data than they were less than a year ago. But it also revealed that the collaboration culture – with widely distributed workforces that use collaboration technologies – is highly productive and here to stay. Security teams must embrace shifts in workplace culture and adapt their Insider Risk strategies accordingly.

Adopt a new approach to data security.

Organizations today are faced with multiple challenges when it comes to building and running Insider Risk programs – including questions about data and program ownership, sub-par processes and tools and anemic budgets. To improve their security posture, organizations must revamp their Insider Risk strategies and directly address existing gaps in their programs.

Invest in modern Insider Risk technology.

To secure the collaboration culture, technology cannot frustrate employees, impede legitimate work and collaboration, force productivity workarounds and leave security teams blind to file movements. As the tide of Insider Risks continues to rise, it is critical for security teams to recast their tech stacks.

Part 6
Methodology

The research for this report was conducted by Ponemon Institute. The survey was completed by 623 IT security leaders and 586 business decision makers from the U.S. All respondents were familiar with their organizations' approach to securing sensitive information.

CODE42

About Code42

Code42 is the leader in insider risk detection and response. Native to the cloud, Code42 rapidly detects data loss, leak, theft and sabotage as well as speeds incident response – all without lengthy deployments, complex policy management or blocking employee productivity. With Code42, security professionals can protect corporate data and reduce insider risk while fostering an open and collaborative culture for employees. Backed by security best practices and control requirements, Code42's insider risk solution 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 backed by Accel Partners, JMI Equity and Split Rock Partners. Code42 was recognized by Inc. magazine as one of America's best workplaces in 2020. For more information, visit code42.com.

Ponemon INSTITUTE

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

We uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.

Contact Us

Code42.com

twitter.com/Code42

linkedin.com/company/code-42-software-inc

US: +1 844 333 4242

CODE42