Insider Risk Management Is Critical To Protecting Valuable Company Data

A Shift Driven By Zero Trust
Insider Risk Management Approaches Are Shifting

Many organizations today are engaging in a Zero Trust security framework, but they ignore the value of data that employees can access and the corresponding insider risk. The pandemic magnified challenges that companies face with insider risk management as employees now access data via new networks and devices, often from their homes.

Security is much more than a technology concern — although it’s often treated as such. Failing to recognize the larger business-continuity impacts that insider risk can have if valuable company data is compromised leaves companies vulnerable and exposed. This research explores how companies are currently treating insider risk management and their changes in strategy for the future.

Key Findings

Insider risk management is of greater concern for 74% of companies now than before the pandemic. As a result, 82% of decision-makers are focused on better protecting company data.

The shift to pursue a more holistic insider risk management strategy is often a part of a proactive (rather than reactive) Zero Trust strategy (59%).

Business leaders agree that a dedicated insider risk program would improve their security posture (76%) and that turning employees into security advocates is a key component of that success.
Pandemic Accelerated Need For Insider Risk Management

It is an absolute understatement to say that security risks have changed drastically because of the pandemic. Three in four decision-makers (74%) say they are more concerned about insider data risk than before the onset of the pandemic. In fact, the top priority of security professionals (82%) is to better protect sensitive company and customer data.

To tackle this, organizations are finding new approaches to protecting data, including protecting against internal breaches via insider data risk management.

74%

We are more concerned about insider data risk than before the onset of the pandemic.

82%

It is a priority to better protect sensitive company and customer data in the next 12 months.
Strategy Shift Attributed To Zero Trust And Workforce Needs

The driving force behind the shift in insider risk strategy spans workforce, partners, tools, and the move to Zero Trust. With heightened adoption of a Zero Trust security framework, 59% have realized the need to pursue more holistic insider data risk management as part of their Zero Trust strategy. Rather than simply trying to prevent threats, Zero Trust requires firms to design security from the inside out — calling for a shift in overall thinking about security and risk and increasing focus on insider risks.

The adoption of Zero Trust, along with an increasingly remote workforce, insider threat incidents, and expanded use of third-party vendors, have pushed decision-makers to focus more heavily on insider risk management as the risks posed by insiders manifest in new ways since the pandemic.

Zero Trust requires firms to design security from the inside out.

Factors That Changed Approach To Protecting Data From Insider Data Risk In Last 12 Months

- **Strategy**: 59% As part of a Zero Trust strategy adoption
- **Workforce**: 70% Increased % of workforce working remotely 65% Insider threat incident
- **Partners**: 65% Increased use of external vendors
- **Tools**: 60% Increased use of decentralized collaboration tools 50% Expanded bring-your-own-device (BYOD) policies

Base: 202 security professionals in the United States who are highly involved with their companies’ data loss prevention and/or data breach mitigation strategies and planning
Source: A commissioned study conducted by Forrester Consulting on behalf of Code42, February 2021
Insider Data Leaks Remain High As Data Leak Prevention Strategies Prove Ineffective

Insiders at a company span beyond just end users; they also include users, partners, and vendors with access to systems and data. Insider risk has become a greater concern since the start of the pandemic, and traditional mitigation strategies have become ineffective. In fact, 66% of respondents still say they experience data leaks due to insiders at least monthly, if not more frequently. Nearly three-quarters (71%) agree that the traditional approach to data leak prevention isn’t working, furthering the shift to a more holistic security program.

Frequency Of Data Leaks Due To Insiders

- Weekly: 5%
- Biweekly: 20%
- Monthly: 41%
- Quarterly: 25%
- Annually: 8%

Base: 202 security professionals in the United States who are highly involved with their companies’ data loss prevention and/or data breach mitigation strategies and planning
Note: Percentages do not total 100 because of rounding
Source: A commissioned study conducted by Forrester Consulting on behalf of Code42, February 2021
Tool And Policy Complexity Creates Hurdles For Insider Risk Management

Although companies are reprioritizing their focus on insider risk, roadblocks stand in their way. Companies are bogged down by too many disconnected tools (75%), managing false positives (71%), and complexity of policy creation and deployment (67%). These hurdles greatly prohibit their insider risk reduction efforts, exposing them to great risk. Rather than being buried with too many false positives and security alerts, a more holistic insider risk security approach as part of a Zero Trust strategy would shift companies from being reactive to threats to proactively identifying insider risks — reducing this complexity and the number of false positives. This reduction in complexity would allow security professionals to focus on risks that truly need their attention, rather than being distracted by too many alerts.

Top 5 Challenges When Protecting Data From Exposure And Exfiltration Risk By Insiders

(Showing percent who label these as “Very” or “Extremely Challenging”)

- Complexity of too many disconnected tools: 75%
- Managing false positives/too many security alerts: 71%
- Complexity of policy creation/deployment: 67%
- Increased administrative load to manage and maintain the solution: 64%
- Abundance of false positives from security software: 62%

FORRESTER OPPORTUNITY SNAPSHOT: A CUSTOM STUDY COMMISSIONED BY CODE42 | MARCH 2021

Base: 202 security professionals in the United States who are highly involved with their companies’ data loss prevention and/or data breach mitigation strategies and planning

Source: A commissioned study conducted by Forrester Consulting on behalf of Code42, February 2021
Dedicated Insider Risk Program Would Improve Protection Posture

Because insiders use data and system access as part of their everyday jobs, it’s difficult to find risky insiders who may pose a threat. The shift to remote work further complicates this. While many decision-makers (64%) prioritize implementing a consistent process to identify and prevent threats, only half (49%) prioritize building a consistent process to identify risk within their organizations, leaving companies exposed.

As a result of insider threat risks, seven in 10 respondents (72%) say their firms will create a dedicated insider threat capability and/or team in the next 12 months to focus on finding and addressing risky insiders. Three in four (76%) agree that a dedicated insider risk capability would improve their overall data protection posture and maturity.
Insiders Prove To Be Valuable Security Advocates

Holistic insider risk management turns insiders into data security advocates (71%). Employees complain that security policies hinder productivity and collaboration (51%) or block them from using data within policy (41%). These frustrations discourage them from embracing security measures.

Rather than hindering, successful security programs embrace employees as security advocates to support safe data handling and computing use. Over the next year, firms plan to create dedicated insider threat teams (72%) and increase security awareness among employees (64%) to embrace the employee perspective. The implications of not creating dedicated insider threat teams are damaging: increased risk and being left behind by competitors. Ideally, companies will trust employees to do their jobs, using tech to empower rather than victimize them.

Insiders Become Security Advocates

- 71%: Effectively turning employees/insiders into security advocates is our current practice for mitigating insider data risk.
- 72%: We are creating dedicated insider threat teams in the next 12 months.
- 64%: We are focused on increasing security awareness among employees in the next 12 months.

Base: 202 security professionals in the United States who are highly involved with their companies’ data loss prevention and/or data breach mitigation strategies and planning.
Source: A commissioned study conducted by Forrester Consulting on behalf of Code42, February 2021
Conclusion

Insiders — employees, contractors, partners, and vendors — have trusted access to companies' most sensitive data and critical systems, posing a potential threat to the business. Instead of treating insiders like criminals, savvy security pros embrace insiders as security advocates and use technology to empower them, protect data, and secure systems.

- Insider risk is hard to find. Because risky insiders have trusted access and know their way around systems, they can be difficult to identify.
- Complexity — including disconnected tools (75%), false positives (71%), and complex policies (67%) — is the enemy. Security pros need processes for addressing insider risk that make it easy to operate and don’t allow risky insiders to flourish.
- Focus is key. A dedicated focus on insider risk helps recognizes risky users before they cause harm.

Project Director:
Emily Drinkwater,
Senior Market Impact Consultant

Contributing Research:
Forrester's Security and Risk research group
Methodology

This Opportunity Snapshot was commissioned by Code42. To create this profile, Forrester Consulting asked custom survey questions of 202 security professionals in the United States who are highly involved with their companies’ data loss prevention and/or data breach mitigation strategies and planning. The custom survey began and was completed in February 2021.

ENDNOTES


ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester’s Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

© Forrester Research, Inc. All rights reserved. Unauthorized reproduction is strictly prohibited. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change. Forrester®, Technographics®, Forrester Wave, RoleView, TechRadar, and Total Economic Impact are trademarks of Forrester Research, Inc. All other trademarks are the property of their respective companies. For additional information, go to forrester.com. [E-50206]

FORRESTER OPPORTUNITY SNAPSHOT: A CUSTOM STUDY COMMISSIONED BY CODE42 | MARCH 2021