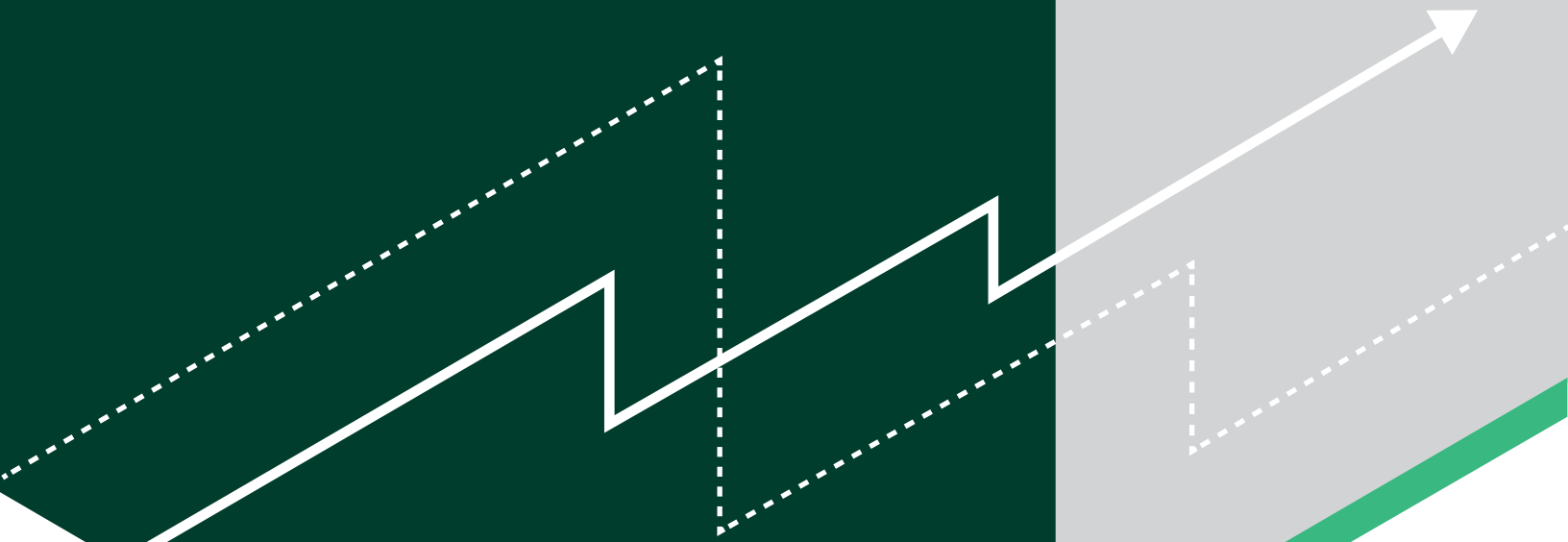
A Forrester Consulting
Thought Leadership Paper
Commissioned By Imperva

December 2021

Insider Threats Drive Data Protection Improvements

Threat Detection, Analytics, And Staffing Lead Investment Priorities



FORRESTER®

Table Of Contents

Project Director:
Madeline Harrell,
Market Impact Consultant

Contributing Research:
Forrester's Security & Risk research group

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.

2021, 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-52036]

FORRESTER®

Executive Summary

Have most organizations come to grips with internal cybersecurity threats? In a word, no, at least not yet. Most firms are taking affirmative steps to protect sensitive data at a time when it is rapidly shifting to the hybrid cloud, but they lack a comprehensive plan that addresses the primary threat.

In September 2021, Imperva commissioned Forrester Consulting to evaluate the way enterprise companies and small and medium-size businesses are protecting their data in response to insider threats as part of a larger response to the globally increased attack surface. Forrester conducted an online survey to explore this topic with 464 managers or executives with data security responsibility primarily in large or very large enterprises. We found that insider threats are not taken as seriously as outsider threats, even though, on average, they comprise more than half of incidents.

KEY FINDINGS

- **Companies struggle to curtail insider threats without a strategic roadmap for data protection.** Fewer than 30% of firms say they have an insider risk management strategy or policy. This deprioritization is manifested by what it's lacking: dedicated team resources, planning, training, and tools.
- **Companies are navigating the changing workforce by making changes of their own: moving to the cloud and making that move securely.** Firms are inexorably moving sensitive data from predominantly on-prem deployments (65%) today to public (40%) or private clouds (77%) over the next two years. This is mainly an economic decision, albeit one with significant cybersecurity strategy implications.
- **Employee productivity and business efficiency improve by adopting technology that is secure and easy to implement.** Today, 44% of firms are hamstrung by difficult and lengthy implementation processes for new data protection technology that doesn't integrate well with existing enterprise solutions.

Protection for companies' intellectual property from internal or external threats must begin at the data layer.

FORRESTER®

Companies Flounder In Cloud Migration Without Proper Data Protection

Sensitive data migrates from on-prem deployments into public or private clouds, and oftentimes organizations will employ a lengthy pit stop in between where the data is held in both cloud and on-prem deployments, i.e., a hybrid approach. Is this migration merely shifting risk from one leaky security channel to another? While nearly two-thirds of firms (64%) believe they have the data solutions and technology in place to scale with their needs, more than half (55%) also say that end users have devised ways to circumvent their data protection policies.

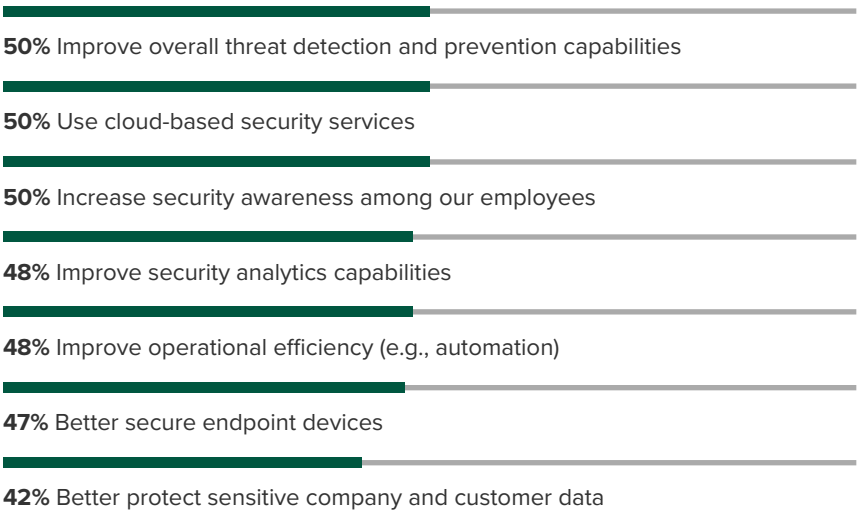
Even without formalizing insider threat plans, firms will prioritize improved threat detection and prevention in 2022 using cloud-based security services and by increasing security awareness at their company. While 35% of firms rely on employees to comply with policies, one-third of firms deploy behavior analytics to detect malicious threats. Nearly half of firms manually monitor or audit employee activity periodically.

That approach may soon become much more scalable. Nearly half of the firms (47%) say they are implementing AI technology for threat intelligence. The move may pay dividends for their incident detection, investigation, and response capabilities as well.

- **Protecting sensitive company and customer data.** The fact that fewer than half of firms (42%) intend to prioritize data protection in 2022 speaks volumes about their multiple and often competing priorities. Leadership realizes the risks of leaving data unprotected, yet it still isn't receiving the appropriate amount of urgency. Either they have become complacent with the processes and tools they already have or they misunderstand how great a threat a breach poses to their business.
- **Seeking speed, firms embrace automation.** Nearly half of firms (48%) will look to gain operational momentum and improve their efficiency with automation, and separately, 35% plan to recruit or hire more in-house security experts. While respondents intend to embrace more modernized modes of operation, they are also throwing headcount at the problem rather than making data-driven, strategic decisions to protect their environment (see Figure 1).

Figure 1

"To what extent is your IT organization prioritizing the following information/IT security goals and initiatives over the next 12 months?"



Base: 464 security and IT professionals with responsibility for managing and responding to insider threats
Note: Showing top seven responses of 13 options
Source: A commissioned study conducted by Forrester Consulting on behalf of Imperva, September 2021

- **"Set it and forget it" insider threat training.** Nearly two-thirds of firms say they train employees to follow data loss policies (see Figure 2), but less than one-third have an insider risk management policy (see Figure 3). This indicates companies have a tendency toward check-box compliance rather than an emphasis on including insider threat risk management at the center of a holistic data loss prevention strategy.

While fewer than one-third of firms have an insider data protection plan, defining policies and identifying data security gaps are common places to start assessing the need.

58% of incidents that negatively impact sensitive data are caused by insider threats.

Figure 2

"Q4-Which of the following tactics does your organization use to ensure that employees comply with your data protection/data loss prevention policies?" (Select all that apply)

65% We train employees to act within our policies.

45% We take disciplinary action on employees who do not comply.

43% We leverage software (like DLP) that automatically blocks data use that does not comply with our policies.

39% We use user analytics to monitor user behavior.

29% We use an SIEM platform to monitor security events.

Base: 464 security and IT professionals with responsibility for managing and responding to insider threats
Source: A commissioned study conducted by Forrester Consulting on behalf of Imperva, September 2021

Figure 3

"How does your organization currently work to protect against unauthorized usage of credentials/insider threats (malicious or non-malicious)?" (Select all that apply)

52% We use encryption.

50% Our IT department manually monitors/audits employee activity on a periodic basis to assess compliance to prevent insider threats.

45% We use database activity monitoring technology.

37% We use DLP technology.

37% We have a dedicated insider threat team.

35% We rely on employees to comply with our policies.

28% We have an insider risk management strategy/policy.

Base: 464 Security/IT professionals with responsibility for managing/responding to insider threats
Note: Showing 7 of 10 responses
Source: A commissioned study conducted by Forrester Consulting on behalf of Imperva, September 2021

FORRESTER®

Companies Fail To Address The Growing Issue Of Insider Threats

You won't see much press or social chatter about insider threats, and few reporting requirements include them. However, almost one-quarter of survey respondents that previously suffered a data breach told Forrester in a study earlier this year that they had experienced at least one insider incident in the prior 12 months.[1] These incidents stem from abuse or malicious intent (43%), unintentional misuse or accident (39%), or both (18%).

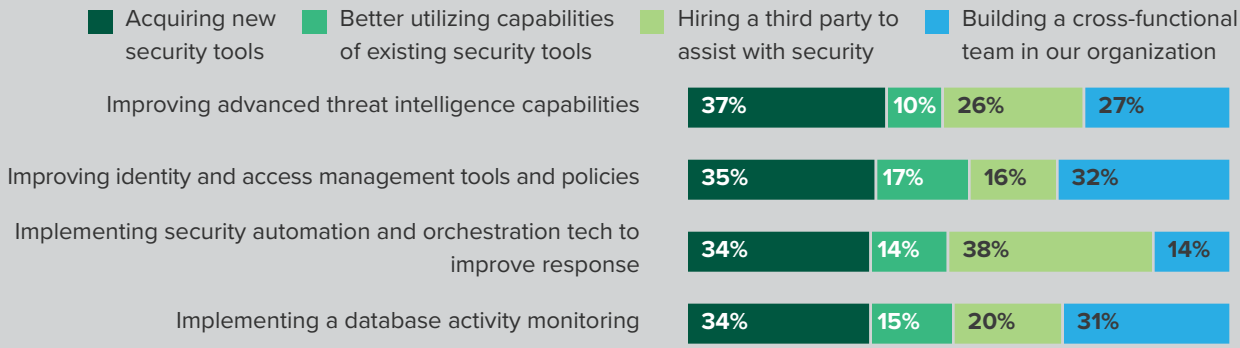
Compromised credentials are among the more problematic insider threat issues, and only 8% of firms said they suffered no policy violations in the past 12 months. Forty-four percent of firms have experienced more than 10 policy violations during that period, spanning late 2020 into 2021.

What are companies doing about the number of policy violations, breaches, and compromised credentials? Most decision-makers are looking to manage this problem with internal resources rather than hire a third party to assist with security. Between 29% to 37% of firms are looking to acquire new security tools to address their current gaps in unauthorized use of credentials (see Figure 4).

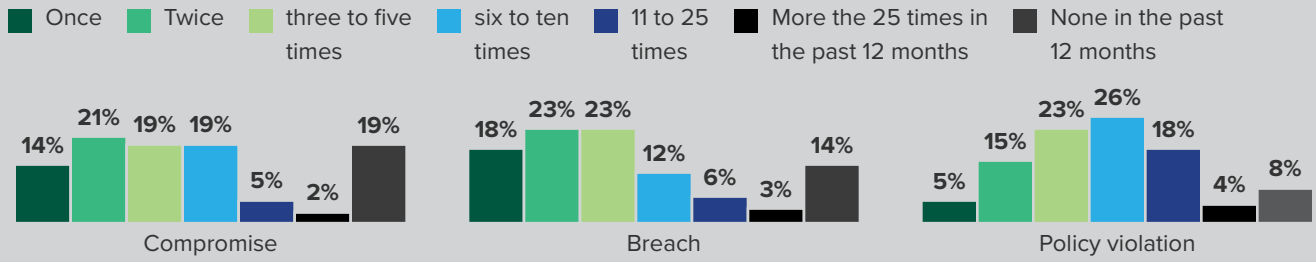
Insider events occur more often than external ones, yet they receive lower levels of investment. That formula seems unsustainable. Today, decision-makers indicate that 58% of sensitive-data incidents are caused by insider threats, compared to 41% caused by external ones.

Figure 4

"How does your company plan to implement the next steps identified in the previous question to address current gaps in unauthorized use of credentials/insider threat capabilities?"



"How many times do you estimate that your organization's sensitive data (e.g., PII, PHI, etc.) was potentially negatively impacted in the following ways in the past 12 months?"



Base: 464 security and IT professionals with responsibility for managing and responding to insider threats
Note: Top chart shows top four responses of nine
Source: A commissioned study conducted by Forrester Consulting on behalf of Imperva, September 2021

FORRESTER®

MOUNTING A VIABLE DEFENSE AGAINST INTERNAL THREATS?

Firms that are not prioritizing insider threat management tend to blame either the lack of internal expertise or the lack of budget for protection. But other problems abound. Nearly a third (31%) of firms do not perceive insiders as a substantial threat, and 30% chalk up their organizational indifference to internal blockers such as executives who do not buy in, sponsor, or champion the cause. Consequently, only 37% of firms have dedicated insider threat teams.

Only 18% of surveyed decision-makers have made increasing spending on a dedicated insider threat program either a rank one or rank two priority in the past 12 months. However, one in four firms (25%) have increased spending on threat intelligence capabilities, which deal with external threats, a rank one or rank two priority in the past year.

Increased spending constitutes four of the six top-ranked responses stemming from incidents in the past 12 months (see Figure 5).

- **Planning for insider risk management hasn't caught on.** Today, just 28% of firms have a risk management strategy or policy. While data theft still matters to them, it points to difficulties managing or coordinating various initiatives. There is less accountability.
- **The cloud is a great place to store or lose sensitive data.** While companies play catch-up, they don't always know what type of sensitive data they're holding or where it is now. Consequently, it is difficult to ensure compliance, and firms consider both issues a rank-one concern, ahead of other policies or visibility.
- **Do data protection policies restrain individual or team productivity?** Around one in three (31%) firms say their employees frequently complain about data protection policies and solutions that hinder productivity and collaboration, blocking them from utilizing data. This perception may complicate obtaining employee buy-in to diminish insider threats.

Figure 5

"What are some of the biggest changes at your organization resulting from the incidents occurring in the past 12 months?"

Base: 464 security and IT professionals with responsibility for managing and responding to insider threats
Note: Showing top six responses out of 10 and showing top three ranks of five.
Source: A commissioned study conducted by Forrester Consulting on behalf of Imperva, September 2021

FORRESTER®

Improve Productivity And Visibility Through Data Protection

Adopting a security tool that protects the data layer as part of a complete data protection strategy yields clear benefits. Increased data visibility is the number one ranked technical benefit for survey respondents, while compliance is the number two ranked technical benefit, and less workload on the security operations center is the number three ranked technical benefit. These preferences are followed by improved time-to-detection and resolution of threats.

Of course, a data loss prevention (DLP) program is not an entire course of action against insider threats. Even organizations that cannot devote the resources to a permanent team can create committees and look for executive sponsorship. Threat analysts may need additional training to understand insider threats, employee-monitoring policies, or privacy rules.

A comprehensive data protection strategy will improve the alignment of teams, reduce insider breaches, reduce negative brand impact, and create cost savings from fewer security events.

- **A comprehensive data protection strategy drives better security culture within the business.** A comprehensive data protection strategy would not only save the business the headache and cost of continued regular security events, but it would also foster internal collaboration among internal teams. More than half of the respondents (53%) have experienced or would expect to experience improved alignment across security, IT, legal, leadership, and other teams due to having a comprehensive data protection strategy. Likewise, over one in four (43%) decision-makers associate a comprehensive strategy with cost savings from fewer business-impacting security events.
- **Data protection means fewer breaches and better brand protection.** Nearly half of firms (49%) believe that a comprehensive data protection strategy will lead to fewer internal data breaches or security events that come from an unauthorized use of credentials. Though they're not the same thing, improving data protection helps advance the cause. While companies can expect a reduction in internal data breaches and fewer business-impacting security events, they can also expect reduced negative impact on brand reputations (45%). With fewer incidents to rattle consumer trust, brands solidify their good standing with customers (see Figure 6).
- **Improving scalability with business needs is a priority.** Nearly half of firms say that implementing technology or a service that protects the data layer will improve scalability with business needs. It's a safe bet that business needs will surely change, and security at the data layer will always need to be able to scale with the product.

Figure 6

"What organizational benefits have you experienced/would you expect to experience from having a comprehensive data protection strategy?"

Base: 464 security and IT professionals with responsibility for managing and responding to insider threats
Note: Showing top four responses of seven
Source: A commissioned study conducted by Forrester Consulting on behalf of Imperva, September 2021

Key Recommendations

Insider risk presents a challenge for security professionals who are charged with protecting their organization from cyberthreats and preventing data breaches. Security teams primarily focus on threats coming from outside the organization, leaving them largely blind to threats originating inside. Insider risk is a human problem, not a technology issue, and it must be treated as such. Security teams must create a focused strategy to adequately address insider risk that combines data protection, user monitoring, and a Zero Trust approach to protect against insider threats.

Forrester's in-depth survey of 464 security and IT professionals with responsibility for managing and responding to insider threats at organizations to evaluate the strategies that enterprise companies are using to protect their data yielded several important recommendations:

Add insider risk to your data protection strategy. Add insider risk prevention to your data protection strategy if it's not already included. If your plans don't already include insider risk, make it a priority.

Gain stakeholder buy-in for your insider risk program. Senior executives across the company must endorse and support the insider risk program for it to be successful. Start at the top to gain buy-in and sponsorship, then engage with leaders from HR, legal, IT, and other parts of the organization.

Follow Zero Trust principles to address insider risk. The Zero Trust framework for information security was designed to limit access to sensitive data and systems. Following a Zero Trust approach helps protect data and users while limiting the ability of insiders to use sensitive resources not required by their function.

Build a dedicated function to address insider risk. Since insider risk is a human problem and very sensitive in nature, it requires dedicated resources. These may be part of the security team or, better yet, a separate dedicated function. Either way, this team needs a specific mandate for insider risk and training to recognize and respond to insider threats.

Create processes for your insider risk program and follow them. The sensitivity of insider risk and its associated privacy concerns require that strict policies are implemented and followed. Treat every investigation as if it will end up in court and apply policies consistently.

Implement a comprehensive data security solution. A complete solution goes beyond DLP to include monitoring, advanced analytics, and automated response to prevent unauthorized, accidental, or malicious data access. The technologies you deploy should support the processes you've created and the mandate for your insider risk function. Your organization will see cost savings and a reduction of risk from business-impacting security events.

Appendix A: Methodology

In this study, Forrester conducted an online survey of 464 security and IT professionals with responsibility for managing and responding to insider threats at organizations in APAC, EMEA, and North America to evaluate the strategies enterprise companies are using to protect their data. Survey participants included decision-makers in IT, compliance/governance, or security. The study began and was completed in September 2021.

Appendix B: Demographics/Data

GEOGRAPHIES

(Percentages do not add up to 100 due to rounding)

United States	**20%**
Canada	**13%**
India	**11%**
France	**11%**
Japan	**11%**
Germany	**11%**
United Kingdom	**11%**
Australia	**7%**
New Zealand	**4%**

COMPANY SIZE

(Percentages do not add up to 100 due to rounding)

>20,000	**11%**
5,000 to 19,999	**38%**
1,000 to 4,999	**44%**
500 to 999	**6%**

RESPONDENT LEVEL

C-level	**5%**
VP	**9%**
Director	**35%**
Manager	**51%**

INDUSTRY

(Percentages do not add up to 100 due to rounding)

Retail	**17%**
Telecommunications services	**17%**
Financial services	**17%**
Energy, utilities, and/or waste management	**17%**
Healthcare	**17%**
Insurance	**17%**

DEPARTMENT

(Percentages do not add up to 100 due to rounding)

IT	**58%**
Compliance/governance	**29%**
Security	**14%**

Base: 464 Security/IT professionals with responsibility for managing/responding to insider threats
Source: A commissioned study conducted by Forrester Consulting on behalf of Imperva, December 2021

Appendix C: Endnotes

[1] Source: "Best Practices: Mitigating Insider Threat," Forrester Research, Inc., March 18, 2021.