code42

Building a Budget for an Insider Threat Program

5-Step Guide to Demonstrating Business Value and Gaining Executive Buy-In

OCTOBER 2022

As insider threat gets more attention, response still lags behind

Insider threat has been a top challenge in the enterprise security world for years now. But with insider threat incidents making headlines — embarrassing companies and damaging revenue — every week, the issue is catching the attention of more and more C-level executives, and putting new pressure on security teams to do more. There's no question that the problem is getting worse, with the Ponemon Institute reporting that insider threat incidents increased 47% over the last two years — and the costs of those incidents rose by a third.[1] Nevertheless, the majority of business still do not have a dedicated insider threat program in place. What accounts for the gap between concern and response?

The root of the problem is that security teams are already stretched thin. Despite increasing security spending, the widening threat landscape means most security teams barely have enough people, budget, time and attention to go around.

And to ask for more — more budget to implement a new insider threat solution, more staff to manage that solution, more organizational focus on this growing threat — security teams need to build a solid business case and demonstrate the ROI for an insider threat program.

Acting on insider threat: pushing past the tipping point

Scary statistics alone do not make a business case. To convince senior leadership and get top-down buy-in to implement a comprehensive, purpose-built insider threat solution, security teams need to connect the value of that solution not just to risk mitigation, but to added business value. An effective business case needs to explain how an insider threat program can drive operational savings today, free security resources to apply to other strategic initiatives tomorrow, and ultimately unleash the collaborative productivity and innovation that drives competitive advantage in an economy propelled by rapidly evolving ideas.

This eBook outlines a simple strategy for building that business case, focusing on 5 key elements of business value:

1. Mitigating business impacts
2. Reducing existing costs
3. Freeing up internal resources
4. Adding value to your existing toolset
5. Empowering the collaboration culture

1 Mitigating business impacts

The first thing to establish: implementing (or enhancing) an insider threat program will immediately deliver measurable protection to your data and your business. Security directors, all the way up to the C-suite, have increasingly experienced the firsthand impact of insider threat incidents. And if they haven't had the pleasure themselves, they've read about peer organizations in the headlines. But beyond anecdotal examples, you need to make sure all stakeholders and decision-makers recognize the real — and rising — risk. You can make a statistical case with a simple equation:

Why is insider threat increasing?

Increasingly Valuable Unstructured Data

The most valuable and sensitive information in the typical organization is no longer structured, regulated data — it's the source code, design files, product roadmaps, market strategies and sales lists that define a company's competitive advantage. By 2025, 80% of all enterprise data will be unstructured.[3]

+

Increasing Data Portability

It is easier and faster than ever to move data and new technologies — cloud- and web-driven apps — continue to increase data portability. As more organizations migrate their digital infrastructure to the cloud, this data portability makes a giant leap forward. In fact, most security professionals agree that detecting insider threat attacks is harder post cloud migration.[4]

+

Increasing Employee Mobility

People switch jobs more frequently than ever, averaging less than three years with a company.5 With declining tenure comes declining allegiance to an employer: the majority of workers believe they — not their employer — own the ideas and work that they create. And that leads 2 in 3 to say they have taken data with them when they left a job, feeling entitled to do so.[6]

=

Increasing Insider Threat

Employees are hopping between jobs constantly, empowered by new technologies to easily take valuable unstructured data and files with them when they go. So it's no surprise that, even as insider threat awareness rises, insider threat incidents have increased by 47% in the last two years — and show no signs of slowing.[7]

The Takeaway: What will an incident cost your business?

To get your key stakeholders to understand the potential business impacts of an insider threat incident, start by asking these three questions:

1. How are you going to feel when you see the company name in the headlines? How will our customers feel?
2. What will happen if our most valuable and confidential data — our trade secrets and IP — gets out to our competitors?
3. How much will it cost by the time the incident is all over — adding IP litigation, long-term reputation damage and ongoing revenue losses?

2 Reducing existing costs

Right-now business value is always more compelling than maybe-later business value. So, after establishing the potentially devastating business impacts of a major insider threat incident, make the case for how a focused insider threat program will deliver cost savings today.

The reality is that, while they may not be landing your company in the headlines or even getting C-suite attention, insider threat incidents are happening every day in your organization. You're already paying the high price of a reactive approach that yields ineffective monitoring and investigation capabilities. And that cost is increasing rapidly: Overall, insider threat investigation costs rose 86% over the last three years.[8]

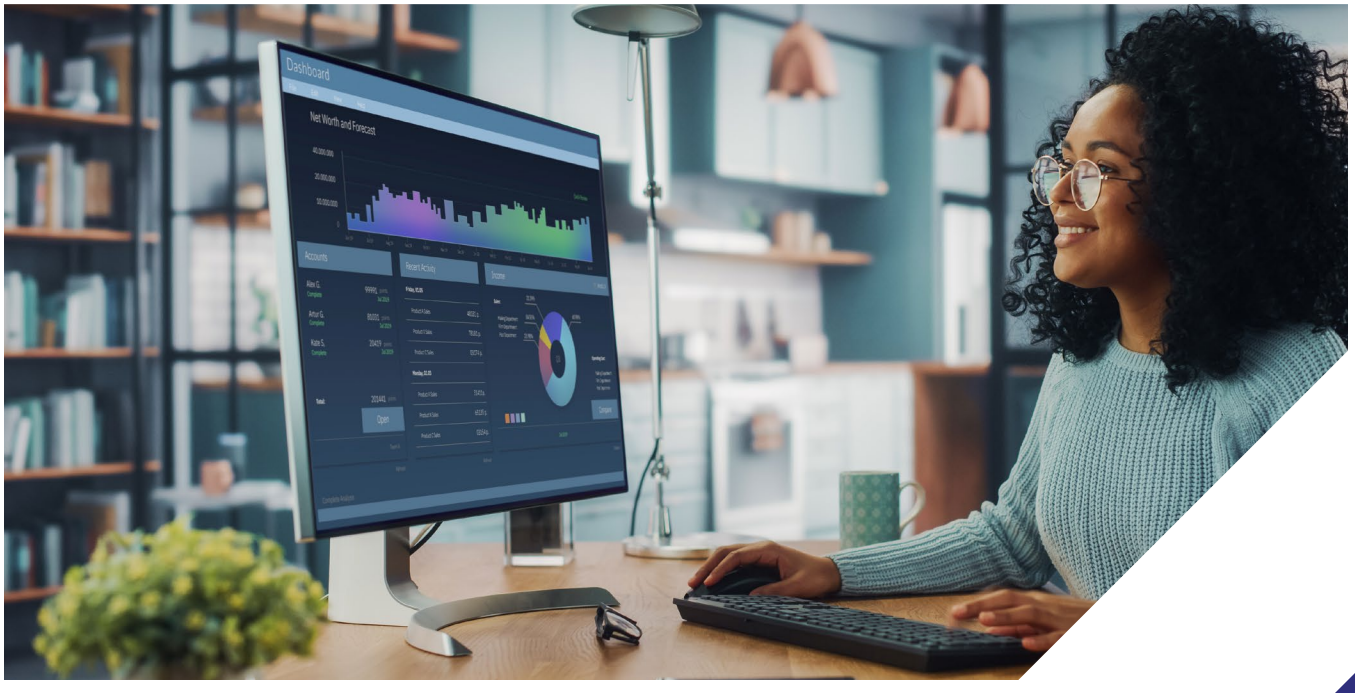
The high cost of ad hoc investigations

For the 80% of organizations that still lack a dedicated insider threat solution, ad hoc investigations are the standard response to suspicious or risky user activity. Because they lack immediate and complete visibility into data activity, investigators have to painstakingly unravel impacted files, external connections, cloud activity, printed documents and much, much more — slowly piecing together the story of (at least some of) what happened. These improvised investigations take an average of 40 hours per investigation per device.[9]

It's easy to get an idea of how these everyday investigations start taking big chunks out of budgets and bottom lines, as more than 60% of organizations report 30+ insider threat incidents in the last year.10 Moreover, a 2020 Ponemon Institute report found that insider threat incidents that took more than 90 days to contain cost twice as much as incidents that were contained within the first 30 days. Time is money when it comes to investigating, but unfortunately, the average insider threat incident takes 77 days to contain.[11]

The Takeaway: Cut investigation time (and cost) by up to 75%

Any stakeholder can quickly begin to add up the enormous costs of a high-profile data breach. But most are unaware that lower-profile insider threat incidents are happening everyday — and they're startled by how much slow, gap-riddled, ad hoc investigations are costing the organization. Here's the simple solution: A purpose-built insider threat solution like Code42 Incydr™ can cut this investigation time by 65–75% from Day 1. That's real, measurable savings — money in your business' pocket — today, and every day from now on.



3 Freeing up internal resources

Cost savings is a benefit that speaks clearly to anyone in the organization. But in the case of driving more efficient security investigations, it's not just the time and cost saved. Faster investigations free up security resources for other valuable strategic initiatives.

Inefficient insider threat response detracts from other security priorities

The fact is that, insider threat isn't a top priority for security teams in many organizations — there are simply more immediate security concerns. Nevertheless, the statistics discussed previously demonstrate that the typical security team is still spending a lot of time monitoring, investigating dealing with false positives from DLP and other conventional prevention tools. Frequently, IT gets dragged into issue resolution — expanding the time and resource drain. These inefficient activities are eating up precious security and IT resources — and not giving the business much value in return. Moreover, as security and IT teams get bogged down in ad hoc insider threat investigations, their attention and time is pulled away from the things that have been identified as a higher business priority than insider threat.

The Takeaway: Rapid investigations are a 3-for-1

By speeding insider threat investigations as much as 75%, a proactive program leveraging a purpose-built insider threat solution like Incydr attacks the resource drain of a reactive, ad hoc approach. In practice, this delivers what any grocery store shopper recognizes as a pretty great value — buy one, get two:

1. Faster, focused investigations deliver cost savings upfront.
2. Security and IT teams get valuable time back to focus on top priorities and strategic initiatives to add additional business value.
3. Faster, focused investigations ensure that the time you do spend on insider threat is well-spent, delivering effective risk mitigation and business protection.

4 Adding value to your existing toolset

As technologies evolve and proliferate across the typical organization, decision-makers are increasingly wary of redundant tools and technologies. One of the most common barriers security teams encounter when trying to gain buy-in for an insider threat solution is the basic, "Don't we already have a tool for that?"

But today, no security tool operates in a bubble. Security technologies and processes are all part of a complex, interrelated security ecosystem. Of course you don't want redundant tools — but you don't want gaps, either.

Filling the gap in the stack

Unfortunately, growing attention on the insider threat challenge has exposed an all-too-common gap in the typical security stack: Conventional prevention tools like DLP and CASB are being applied to insider threat use cases, but these tools were not designed for the unique challenges of insider threat. They struggle to handle the unstructured data that makes up the bulk of trade secrets and IP in modern companies. They struggle to handle the increasing modes of moving data — devices, media, cloud and web apps, etc. And because they are designed to focus on a defined set of data, they are largely blind to any data risk that falls outside their defined scope. A purpose-built insider threat solution like Incydr is designed for the specific challenges of the rapidly evolving, dynamic insider threat problem. In short, an insider threat solution doesn't replace conventional security tools — it complements their functionalities while actually enhancing many of their capabilities, adding the critical visibility needed to rapidly investigate any suspicious or risky action, whether from an insider or otherwise.

The Takeaway: Data visibility makes all your security tools more valuable

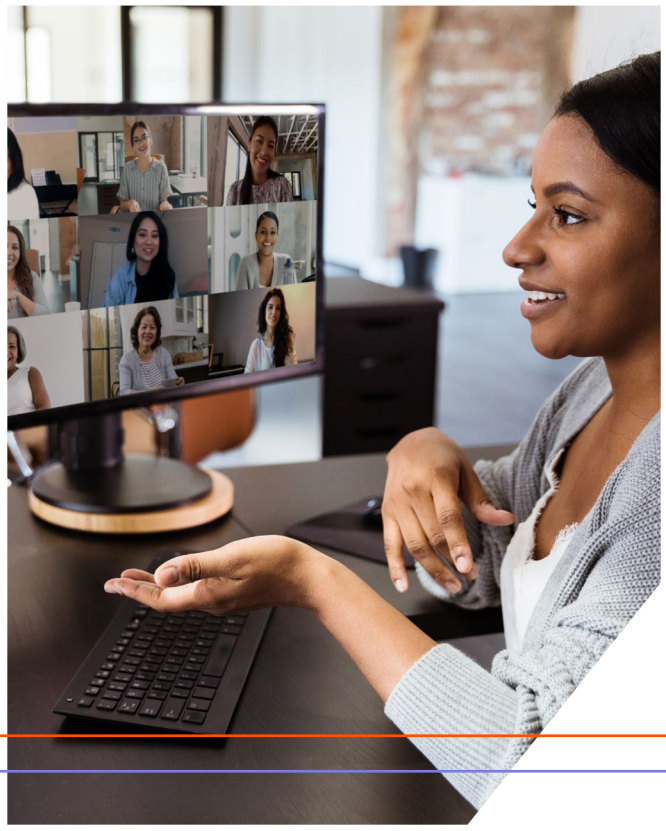
A purpose-built insider threat solution brings its own independent value — which is thoroughly detailed in this eBook. But in another "buy-one-get-one" value, the comprehensive and intuitive visibility offered by an insider threat solution ultimately makes all of your security tools more valuable — and makes your core security workflows more effective.

5 Empowering the collaboration culture

Modern business is defined by its culture of collaboration. Ideas are created, iterated, evolved and advanced as they move between and among employees. Productivity is driven by the ability to connect with colleagues, share information and work in real time — from anywhere, any time, on any device. Business leaders at every level recognize that unlocking and enabling collaborative productivity is critical to driving both bottom-line success and innovative competitive advantages.

Empower your people — or protect your data?

The conventional security toolset was not designed for this paradigm shift, and too frequently ends up impeding productivity and stifling collaboration and innovation. In practice, conventional security tools force security teams to make an impossible choice: empower employees — or protect the data. No matter where on the spectrum they land, this forced trade-off has real costs to the business. You're putting your competitive advantage at risk by inhibiting user productivity and collaboration — or you're risking letting your competitive advantage leak out via insider threat.



A solution built for the collaboration culture

Modern insider threat solutions like Incydr are purpose-built to enable and support the collaboration culture. Rather than trying to block activity, they aim to give security teams visibility and context around data activity, so they can rapidly identify and respond to risky actions. This approach unleashes your employees to do what they do best — work effectively, share easily, iterate and innovate collaboratively — while giving the business the critical protection it needs for its most important, valuable information.

The Takeaway: Empower your people — protect their ideas

You know that your people are your greatest asset. A purpose-built insider threat solution enables you to empower them to use new technologies to work in dynamic, collaborative and innovative new ways — while protecting the valuable ideas that collaborative work creates.

Seeing more — costing less?

The harsh reality is that most organizations are letting far too many insider threats fall through the cracks. The conventional approach— prevention — leaves security teams without the visibility they need to see all their data and catch all the risk activity. Dedicated insider threat solutions like Incydr promise to plug these gaps, giving you visibility to all your data and all your risk, and allowing you to easily home in on the events that matter most. But security teams, as well as other business stakeholders, are naturally skeptical of this. They're already increasing security and IT spending, and security teams are already struggling with alert fatigue, overwhelmed by intensive monitoring and investigations. Adding more rightfully makes people nervous — seeing everything sounds like more work, more complexity, more time and more cost.

Context is key

The key is putting your data in context. A purpose-built insider threat solution like Incydr shows you all your data activity — but it allows you to see that activity through the lens of your biggest insider threat risks: your departing employees, onboarding employees, remote employees, high-value data and high-risk users, and situations like M&A and other organizational change. This focused approach enables the security team to address 90% of insider threats in the typical organization with just a few simple, highly automated workflows. Context is the key that unlocks a bigger "bang for your buck," allowing the security team to see more risk, more quickly and accurately — while actually reducing the time they spend monitoring and investigating.

Immediate impact — Scalable solution

Even with the strongest business case, security teams often run into hard limits on budgets and resources. Because the easy-to-implement Incydr architecture deploys in days, not months (lessening the burden on both IT and security), the solution can be cost-effectively deployed to all users to rapidly deliver comprehensive visibility. But Incydr is also built to enable you to start small, making an immediate impact on your single biggest insider threat risk: departing employees. Once you've deployed Incydr to all users, the Incydr Departing Employee Lens gives you a purpose-built workflow for monitoring, investigating and responding to data exfiltration by departing employees. How big is the departing employee problem?

This enables you to easily build your departing employee workflow and see immediate results. You can leverage this quickly proven impact to gain stakeholder buy-in, confidence and project momentum to continue scaling up to address your other biggest insider threat risks.

Sources

1 Ponemon Institute: 2020 Cost of Insider Threats: Global Report

3 IDC

4 2020 Insider Threat Report

5 U.S. Bureau of Labor Statistics

6 Precision Discovery forensic investigations, 2018 7 2020 Insider Threat Report

8 Ponemon Institute: 2020 Cost of Insider Threats: Global Report

9 Forrester Total Economic Impact Study 2019

10 Ponemon Institute: 2020 Cost of Insider Threats: Global Report

11 Ponemon Institute: 2020 Cost of Insider Threats: Global Report

> Two in three employees openly admit to taking data when they leave a company — and they're taking the data that will serve them best in their future jobs.[12]

Gartner Peer Insights
50+ Verified Security Reviews
★★★★★
4.8 out of 5 stars

About Code42

Code42 is the leader in Insider Risk Management. Native to the cloud, the Code42® Incydr™ solution rapidly detects data loss and speeds incident response without inhibiting employee productivity. Amplifying the effectiveness of Incydr are the Code42® Instructor™ microlearning solution, and Incydr's full suite of expert services. With Code42, security professionals can protect corporate data and reduce insider threats while fostering an open and collaborative culture for employees. Innovative organizations, including the fastest-growing security companies, rely on Code42 to safeguard their ideas.