Making the Case for Insider Risk Management to C-level Execs and the Board

A practical guide for information security leaders

*89% of CISOs believe how employees work puts the enterprise at greater risk of a data breach…*and they're right.

Corporate Data Exposure:

- 63% of employees use unsanctioned applications weekly if not daily
- Thus, 71% of enterprises lack visibility to sensitive data movement
- Making employees 85% more likely to leak data than they were pre-COVID

As executive leaders and Boards foster workforce cultures rooted in speed, the more cloud-based, collaborative and unfortunately compromised the organization's corporate data becomes. We call it Insider Risk and it requires the attention of C-level Execs & the Board - now.

Insider Risk as a result of how employees work, is dynamic and largely hidden from the data protection people, processes and technologies in place today. Protecting data from dynamic risk with technology designed for static risk is a recipe for disaster.

Why organizations are at greater risk:

- **Risk is hidden.** 63% of security teams indicate they lack the needed context to prioritize the data risks that matter most to the business.
- **Tech is outdated.** 91% of security teams say they lack the purpose-built technology to effectively & efficiently manage Insider Risk.
- **Time is wasted.** According to security leaders, it takes nearly six months to identify and contain an insider data breach – that's two business quarters at risk.

In this paper, we outline how security leaders can make the case to C-level Execs and the Board for the budget and resources needed to address the growing corporate data leak problem that is Insider Risk.

How to make your case:

- Qualify when your organization is most exposed by focusing on the major Insider Risk triggers
- Qualify where your organization is exposed and identify the gaps in security people, process and technology
- Quantify how your organization's exposure impacts market position, revenue and brand value

Figure 1: Insider Risk to corporate data - When, where, how it manifests and what won't you tolerate

Qualify when organizations are exposed?	**Product Launch, Customer Deals, Partner Contracts**	**Pre/Post Merger or Acquisition (M&A) or IPO**	**Pre & Post Leader & Org Change, Layoffs**	**Pre & Post Culture, Tech, Policy Changes**
Qualify where organizations are exposed?	**Privileged Access Credential Gaps**	**Security Policy & Compliance Gaps**	**Security Awareness & Training Gaps**	**Shadow IT & Mirror IT Usage Gaps**
Quantify how organizations are exposed?	**Unauthorized Employee & Contractor Access**	**Employee & Contractor High Risk Behavior**	**On-boarding & Off-boarding Employees & Contractors**	**Employees & Contractors Remote & Hybrid Work**

Qualify when your organization is most exposed by focusing on the major Insider Risk triggers

The measure of an organization's success is often measure in reward and time. Most organizational strategies, plans, priorities and metrics are rooted in a "time to reward" mindset. This is how decisions get made. Time to market, time to revenue, time to value are all intrinsic to nearly every decision made at an organization – including how employees get their day to day work done. This is evidenced by Code42 Data Exposure Report findings over the past year:

- 63% of employees use unsanctioned applications weekly if not daily
- Thus, 71% of enterprises lack visibility to sensitive data movement
- Making employees 85% more likely to leak data than they were pre-COVID

What is seldom factored into the decisions employees make is risk – what we call Insider Risk - data exposure events whether they be security, compliance or competitive in nature - that jeopardize the financial, reputational or operational well-being of a company and its employees, customers and partners. In order to effectively manage Insider Risk, we suggest organizations focus on when the risk to the organization is highest – when there is the most to lose relative to market position, revenue or valuation.

Insider Risk to corporate data is often triggered and/or elevated at times of organizational change. Organizational change can often drive employee uncertainty. Employee uncertainty leads to anxiety, and increased employee anxiety results in increased potential for Insider Risk - corporate data exposure, leak and breach.

Here are a few examples of organizational change that happens across organizations of all sizes – some more frequent than others. C-level Execs and Boards need to weigh not only the time and reward of such changes, but the risks they introduce to the business and if security is adequately equipped to prevent them.

Pre/Post Merger or Acquisition (M&A) and Initial Public Offering (IPO)

Mergers and acquisitions (M&A) elevate the risk of corporate data loss and theft. Not only do they commonly trigger employee reorganizations, redundancies and layoffs, but employees of the sell-side company may leave voluntarily due to worries about their job security. Imagine a scenario where a high-tech startup was acquired for its innovative software. Reorgs are announced, layoffs are rumored, and recruiters begin to target the software developers with a large compensation package. A developer takes the new job and transfers some source code to his personal cloud account thinking it will be useful in his new role. This loss of such IP, which represents much of the value of the M&A, is a dealmaker's nightmare. The same can be said for data leaks pre/post an Initial Public Offering (IPO). Imagine if the organization's secret sauce, their trade secrets, their crown jewels leaked prior to IPO or shortly after IPO – the impact could be devastating to investors and shareholders, not to mention the long-term effect of brand and reputation damage.

Pre & Post Leader & Org Change, Layoffs

Changes in executive leadership and/or restructuring efforts is a common organizational change, but changes at the top and reorgs put corporate data at increased risk. When leaders changes and employees move to new teams or inherit additional job responsibilities, they gain access to new information and systems. Additionally, such change can generate new risk factors. Employees may become a flight risk if they dislike their new leader or job. They may also worry that leadership change or a restructuring will result in a layoff due to job redundancies. Like leadership changes and reorgs, layoffs also increase insider risk to corporate because they are often rumored before they're announced. Many will begin proactively searching for jobs because they fear for their financial security, and take corporate files they believe will help them while they're at it. Additionally, layoffs result in many departing employees at once which is overwhelming for security teams who must ensure data remains protected. Not only are these departing employees more likely to take data with them when they leave, but they are more likely to be hurt and angry. Some may even wipe their computers clean and delete important work on their way out.

Pre & Post Culture, Tech, Policy Changes

The ever-changing dynamics of corporate culture, technology and the need to evolve corporate policies is often a trigger for insider risk. As organizations shifted to remote work during the onset of COVID-19, the likelihood of employees leaking corporate data nearly doubled (85%). Now, as organizations ponder and plan their policies for a hybrid workforce or a return to the office, employees are also pondering and planning whether they stay or go. The same can be said when sweeping technology changes take place. As organizations shift from on-premises software to cloud services or shift from one cloud subscription service to another – nearly annually – this too introduces uncertainty and risk. With each and every cultural and technology change, no doubt corporate policies change with them.

Product Launches, Customer Deals, Partner Contracts

In fast moving organizations where time to market, revenue and value are paramount, employees are creating, sharing, and moving data every second of every day. The hidden risk in time sensitive projects like product launches, pending customer deals and partner contracts (think supply chain) is what happens if the information gets out i.e. goes public prior to the pending announcement? Factoring risk into your decision making process forces you to ask "what if" questions. What if your organization is working on a super secret product that would be game changing not only for your business but the market at large? What if you are on the brink of landing a major customer and your sales proposal leaks to another supplier in the running for the client's business? What if you are inking a new contract with a supplier that includes strategic pricing or logistics? Information related to any of these "what if" scenarios that falls into the wrong hands be it a competitor, client or the media will make or break your organization's time to market, revenue and value. That is why it is imperative that the security team understand such organizational milestones and the risk tolerance that goes with them. Such foresight enables security teams to proactively put into place the people, process and technology to prevent Insider Risk from negatively impacting market position, competitive edge and brand value.

Qualify where your organization is exposed and identify the gaps in security people, process and technology

For your security team to proactively put into place the right people, process and technology to prevent Insider Risk, you first must know where you have potential gaps. No doubt, your security team has put in place data policies, governance and controls in order to prevent data leak and theft i.e. Insider Risk. But, in times of heightened data sensitivity (the triggers mentioned in the previous section) and thus, lower data risk tolerance, C-level and Boards want assurances. Assurances that data use policies are being followed and data governance and controls are effective. Simply assuming policies are being followed and your processes and technology are effective creates a false sense of security and with it material risk to market position, competitive edge and brand value.

Knowing your organization's Insider Risk exposure starts with having zero trust in the technology you have in place when it comes to data security. Never trust, always verify is critical to meeting the C-level and Board's demands for assurances – especially when the organization's valuation is at stake. To create assurances start by recognizing where gaps exist. Gaps in privileged access, policies and compliance, employee awareness and training and employee Shadow IT and Mirror IT usage is a great place to start. To do so, conduct a quick assessment by monitoring all user activity, file movement and the vectors or destinations said files are moving to. If nearly two-thirds of employees use unsanctioned applications weekly if not daily to get their jobs done, odds are sensitive corporate data is moving to and through these applications. In order for security to be adequately equipped to prevent corporate data leaks at times of lowered risk tolerance, you need to know where to start. Where do you trust sensitive data be stored and who should have access? More importantly, what are the untrusted destinations sensitive data is moving to and who is moving it there?

Answering these fundamental questions arms security and the organization at large to ensure they not only put the right policies, governance and controls in place, but create assurances a sensitive data leak does not introduce material risk to a product launch, customer deal, partner contract, M&A, IPO, organizational change or technology rollout.

For more information on how Code42 Insider Risk Management provides you the assurances you need, here are some helpful resources to browse:

- **About Code42 Insider Risk Management**
- **5 simple steps to get started with Insider Risk Management**