BRC
BOARD RISK COMMITTEE
BOARD RISK REPORT

*"Not every insider risk becomes an insider threat; however, every insider threat started as an insider risk." (1)*

September 26, 2022

# Stepping Up – The Board's Role in Confronting Insider Risk

By Linnea Solem

When board directors first hear the term "insider risk," their initial thoughts may focus on insider information related to company financials, illegal stock trading, or the selling of company confidential information. In reality insider risk is broader and more nuanced – it encompasses the protection of all company assets including intellectual property, trade secrets, product information, competitive analysis, M&A activity, and even something as basic as existing customer lists.

Last month's BRC *Board Risk Report* provided insights on Integrated Risk Management (IRM), which is the set of practices and processes supported by a risk-aware culture and enabling technologies. This edition puts the spotlight on the other IRM – Insider Risk Management. September is National Insider Threat Awareness Month (2), a collaborative effort between five federal agencies and task forces to raise the awareness around a set of rapidly growing insider risks that warrant board scrutiny now more than ever before.

Insider Risk Management aims to minimize the impact from risks that are driven by internal events and user activities. Gartner defines insider risk management as the tools and capabilities to measure, detect, and contain undesirable behavior of trusted individuals within the organization. An insider threat is anyone with authorized access who wittingly or unwittingly harms an organization through their access to information. In today's extended enterprise, trusted individuals can be employees, partners, or employees of service providers.

---

## INSIDER RISK MANAGEMENT (IRM): DO WE KNOW OUR RISKS?

Insider risk does not require malicious intent. In fact, independent research from the Ponemon Institute showed that 56% of insider incidents were due to the negligence of employees or contractors. Insider threats can stem from careless or malicious or compromised credentials. There is a direct correlation between the size of the organization and the number of insider events. Large organizations manage thousands of internal users, millions of data files, and a vast inventory of third-party relationships.

The hybrid environment adds complexity to gaining visibility to insider threats. The pandemic accelerated the shift in the workforce environment from largely in-office to entirely virtual and now to a still evolving

hybrid environment. The shift toward a work-from-anywhere environment required changes in the granting of remote access privilege, making it more difficult to differentiate insider threats from external attacks. Knowledge workers continue to be the area of the workforce that primarily perform their job in a hybrid or remote capacity. Exploding use of IoT devices, mass migration to cloud service providers, and today's extended network environment require stronger analytics to identify potential insider activities before information is compromised or escapes the company's control.

In the recent Ponemon survey 63% of respondents said they are worried about unmanaged IoT devices resulting in the loss of sensitive data, more than any other channel (3). The overwhelming majority of companies have un-inventoried IoT devices creating significant risk exposure be they printers, online thermostats, or any other company owned device (4). Workers are using personally owned devices and third-party tools for productivity and collaboration, creating an expanded set of endpoints to monitor. Accidental data disclosures and the risk of credential theft requires the capability to analyze information transfers for authorization of both the sender and recipient of company data. External threat actors are using more sophisticated techniques to manipulate information and use online social engineering to gain access to insider information or credentials.

**Questions Boards Should Ask to Assess Insider Risk:**

- Does our organization define and categorize insider incidents or events as part of its existing security incident program?
- Has management defined how to secure work practices over the long term for a hybrid workforce?
- Does our organization classify security events to identify root cause? (e.g., negligence, criminal intent, or credential compromise?
- Does our organization inventory and monitor all company owned IoT devices? Are those devices properly protected?
- Do the firm's acceptable use policy and procedures for use of personally owned devices enable the organization to deploy and leverage employee monitoring tools transparently?

---

**THE PEOPLE COMPONENT: MITIGATING INSIDER RISK IN THE TIME OF THE GREAT RESIGNATION**

Protecting intellectual property must be a top priority in today's business environment. Inadvertent action by employees, direct contractors and supply chain partner staff can subvert protection efforts as much as intentional actions motivated by theft or sabotage. Employers have faced growing challenges not only hiring talented workers but retaining productive employees. Unhappy departing employees can trigger insider risk by taking confidential information to their next gig; and organizations receiving information from new employees can be at risk of product tainting.

Since the pandemic, one in three medium-to-large U.S. companies have adopted some type of worker surveillance system. A downside of such tools is the potential of blocking productivity and increasing employee disengagement. In today's post pandemic environment, more workers are focused on promoting a healthy work/life balance. Disengaged workers may be at a higher risk of resignation or demonstrate a declining level of work ethic. The concept of "Quiet Quitting" where once productive employees do the minimum necessary in their job may be more likely to cross the line into careless behaviors, resulting in increased insider threats. According to a recent Gallup poll (5), at least half of the U.S. workforce is Quiet Quitting and the ratio of engaged to actively disengaged workers is the lowest in almost a decade. Proactive manager engagement strategies like having one meaningful conversation per week with each team member, even if virtual, can aid organizations in improving engagement and minimizing accidental events.

**Questions Boards Should Ask of Their Human Resources and Legal Partners**

- Has the organization taken steps to reskill management to actively promote engagement with employees?
- Does management have procedures in place to address the potential insider threat from departing employees?
- Does the company's Training and Awareness Program include education specific to insider risk?
- Do management policies for the onboarding of new employees contain information to prevent bringing intellectual property of their former employer into the organization?
- Do the firm's onboarding and exit/termination procedures communicate expectations for protection of intellectual property?

---

## INTELLIGENT MONITORING TECHNIQUES ENHANCE INSIDER RISK MITIGATION

Despite recent headlines that have focused on the negative consequences of the use of workplace productivity employee monitoring (6), organizations recognize the need to address the techniques, that when done right, can be useful in identifying and managing insider threats. Federal agencies with access to classified information have been required to have insider threat prevention programs for more than a decade. An increasing number of organizations utilize insider monitoring programs to guard against internal threats. Implemented with transparency and in a way that conforms to corporate values, organizations can leverage data they may already collect.

Securing work practices in today's environment is not just about technical controls but enhancing the risk intelligence of monitoring solutions. Insider Risk Management provides risk intelligence that analyzes and correlates the appropriateness of information sharing between internal senders and intended recipients. Risk monitoring tools can even alert the company to potential credential theft by analyzing the patterns of information sharing. Insider risk management technologies aggregate and consolidate event data already collected by IT systems but enable earlier visibility to the risk of a potential event so that the organization can take proactive steps.

A company's risk culture defines the shared values and beliefs that shape attitudes toward risk-taking. Organizational culture determines how openly risk and losses are reported and discussed. Effective insider risk management programs start by identifying the types of data events or insider actions that can create harm to the organization. These potential harms can be risk rated or graded based on risk severity. Employees in high risk or data-centric roles may require more proactive monitoring of data access, data use, and data transfers.

The potential risk of an insider event grows for departing employees. For departing employees, the risk associated with loss or theft of intellectual property is critically important. In fact, research shows that there is a one in three chance any company will lose IP when an employee quits. Further, three fourths of survey respondents didn't know what or how much sensitive data departing employees take to other companies (7). HR and Legal functions are important stakeholders in developing an Insider Risk Management Program by ensuring transparency, employee notice, and by conveying compliance expectations and misuse consequences in HR policies.

While cybersecurity continuous monitoring tools focus on external monitoring to identify risk, insider risk management tools look internally at events. An internally focused continuous monitoring approach to insider risk can identify patterns or changes in worker behaviors that may indicate a potential malicious

threat. Insider risk monitoring tools can trigger alerts to potential actions prohibited by an organization's compliance and ethics program. Early awareness of these insider events enables informed risk-based decisions.

**Questions Boards Should Ask:**

- Does management ensure that HR policies address transparency and notice not only for acceptable use but for any mechanisms used for employee monitoring, surveillance, or activity tracking? Is management properly sensitive to employee feedback on employee centric workplace monitoring?
- Has management implemented information security and threat management programs to address the risk of credential compromise by employees or third parties?
- Does the organization maintain and regularly communicate company policies and expectations for employees that: limit access to certain categories of websites; contain guidelines on the download or upload of company data; and restrict transfers of company data to unauthorized third parties?
- Do existing policies address the risks associated with a hybrid workforce and/or virtual vendors?
- Has management properly assessed the needs for expanded monitoring solutions to improve detection and analysis of insider risks and threats?

---

**REFERENCES**


1. Gartner Research, Market Guide for Insider Risk Management Solutions, April 2022 https://www.gartner.com/en/documents/4013691
2. September is National Insider Threat Awareness Month (NIATM), which is a collaborative effort between the National Counterintelligence and Security Center (NCSC), National Insider Threat Task Force (NITTF), Office of the Under Secretary of Defense Intelligence and Security (USD(I&S)), Department of Homeland Security (DHS), and Defense Counterintelligence and Security Agency (DCSA) to emphasize the importance of detecting, deterring, and reporting insider threats. https://www.cisa.gov/uscert/ncas/current-activity/2020/08/31/national-insider-threat-awareness-month
3. https://www.proofpoint.com/us/resources/threat-reports/cost-of-insider-threats, page 34. Cloud and networks were the second and third most cited channels of potential insider-driven data loss.
4. https://www.ponemon.org/research/ponemon-library/security/the-internet-of-things-iot-a-new-era-of-third-party-risk.html
5. https://www.gallup.com/workplace/398306/quiet-quitting-real.aspx
6. https://www.nytimes.com/interactive/2022/08/14/business/worker-productivity-tracking.html; https://www.wsj.com/articles/more-bosses-are-spying-on-quiet-quitters-it-could-backfire-11663387216; https://www.advisory.com/daily-briefing/2022/06/29/employee-monitoring
7. https://www.code42.com/resources/reports/2022-data-exposure


---

**RESOURCES**

- https://www.dni.gov/index.php/ncsc-features/2834-september-2021-is-national-insider-threat-awareness-month
- https://www.dni.gov/index.php/ncsc-newsroom/item/2320-ncsc-and-federal-partners-focus-on-countering-risk-in-digital-spaces-during-national-insider-threat-awareness-month-2022
- https://hbr.org/2022/03/the-great-resignation-didnt-start-with-the-pandemic
- https://www.gartner.com/en/documents/4013691
- https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-know-the-risk-raise-your-shield/ncsc-awareness-materials

## ABOUT THE AUTHOR

**Linnea Solem**
CEO, Solem Risk Partners, LLC
Shared Assessments Advisory Board Member

Linnea Solem is CEO and Founder of Solem Risk Partners, LLC a management consulting and advisory services company focused on Privacy Program Management, Third Party Risk Management, and Enterprise Risk Management. She is a management consulting executive and former Chief Privacy Officer and Vice President Risk/Compliance for a large diverse technology service provider. She has a cross-functional background with 30+ years of experience working in regulated industries. She has over 20+ years of experience working with Executive Management and Audit Committee/Board of Director expectations for public company controls and service provider relationships. Her focus is on helping clients navigate the risk landscape with confidence. Linnea and her firm were recently recognized as one of the "10 Best Entrepreneurs of 2020" by Industry Era Magazine.

Linnea is designated a Fellow of Information Privacy (FIP) from the International Association of Privacy Professionals. She maintains her Certified Privacy Manager Certification (CIP/M); Certified Information Privacy Professional (CIPP/US and CIPP/C) for the U.S. and Canada. She is a founding holder of the CTPRP certification for third party risk and is a Certified Third Party Risk Assessor (CTPRA).

---

***The Board Risk Report*** *is the periodic publication of the BRC.* ***SUBSCRIBE NOW*** *to receive complimentary world-class risk management practices delivered directly to your inbox.*

## WHO WE ARE

The Board Risk Committee (BRC) is the foremost thought leadership peer council for board risk committee members and chief risk officers. The BRC is a nonprofit, non-competitive, trusted place for the exchange of ideas, strategies, and best practices in enterprise risk oversight. We advocate for having risk committees of boards, where appropriate, and for educating board directors about enterprise risk. The BRC aims to foster more effective risk management and board oversight. The BRC is affiliated with The Santa Fe Group (SFG) and Shared Assessments (SA). SFG is a strategic advisory company providing expertise to leading corporations and other critical infrastructure organizations in the area of risk management. SA is the thought leader and provider of tools, education and certifications in the third party risk management space. *The Board Risk Report is the periodic publication of the BRC.*

**Contact:**
Catherine A. Allen, Founder, Chairman, Board Risk Committee, cathy@santa-fe-group.com
Ellen Dube, Executive Director, Board Risk Committee, ellen@boardriskcommittee.org