The ROI of Insider Risk Management

This session explored how corporate security teams can demonstrate business value through insider risk programs, moving beyond traditional ROI concepts. Speakers shared practical lessons from building programs at scale, emphasizing risk quantification, monetization of incidents, and stakeholder alignment. The discussion highlighted how metrics, when tied to financial impact, improve executive buy-in, guide prioritization, and strengthen cross-functional collaboration, particularly with HR, legal, and business unit leaders.

Speakers

Paul Force
Senior Director Insider Risk Management
Dell Technologies

Tim Kirkham
Vice President Investigatiosn Practice
Ontic

Key Themes and Topics

Business Value Over Traditional ROI

Security leaders must distinguish between ROI and broader business value. Programs gain traction when framed in terms of protecting revenue, competitive advantage, and reputation. This shift enables more meaningful executive conversations and aligns security outcomes with business priorities.

Monetization as a Strategic Lever

Quantifying insider risk in financial terms transforms perception. By assigning estimated monetary value to prevented losses, security teams move from cost centers to strategic contributors. This approach increases leadership engagement and justifies sustained investment in programs and tools.

Contextual Risk Modeling

Effective programs combine impact and likelihood to produce realistic risk estimates. Applying multipliers based on employee context, such as departure type or intent, creates defensible and credible metrics that resonate with finance and legal stakeholders.

Continued on next page

Key Themes and Topics

Stakeholder Alignment is Industry-Specific

Successful programs depend on aligning with the right internal partners. These vary by industry, such as engineering, legal, or operations. Understanding who owns value in the business is critical for accurate risk assessment and long-term program adoption.

Metrics as Operational Intelligence

Metrics serve more than reporting. They help identify high-risk behaviors, guide targeted interventions, and optimize resource allocation. When analyzed effectively, they enable proactive risk reduction rather than reactive investigation.

Actionable Takeaways

Define High-Risk Behaviors First

Start by identifying specific employee behaviors that present the greatest risk, such as offboarding or workforce reductions. Focusing on defined scenarios allows faster implementation, clearer measurement, and early wins that build program credibility.

Build a Simple Risk Valuation Model

Develop a consistent framework combining estimated business value and likelihood of misuse. Use conservative multipliers to maintain credibility. Collaborate with finance and legal early to ensure alignment and avoid future challenges in interpretation.

Engage Business Unit Experts for Valuation

Work directly with subject matter experts to estimate the value of sensitive data. Provide structured guidance to help them quantify impact. This ensures valuations are grounded in operational reality and defensible to leadership.

Strengthen Cross-Functional Partnerships

Actively collaborate with HR, legal, and IT to expand visibility into risk signals such as performance plans or workforce changes. Strong partnerships unlock better data, improve response coordination, and enhance program maturity.

Continued on next page

Actionable Takeaways

Use Metrics to Drive Targeted Interventions

Analyze trends to identify high-risk teams, regions, or roles. Deploy focused training and controls where risk is highest. Measure impact over time to demonstrate effectiveness and continuously refine your approach.

Strengthen Cross-Functional Partnerships

Actively collaborate with HR, legal, and IT to expand visibility into risk signals such as performance plans or workforce changes. Strong partnerships unlock better data, improve response coordination, and enhance program maturity.

Notable Quote

> **In the corporate world, you're not really there to catch bad guys. We don't have bad guys. We hire good people and our job is actually to keep them good people and help them make good decisions as they transition through the life cycle of employment at that company.**

- Tim Kirkham
Vice President Investigations Practice, Ontic

Final Message

Corporate security programs succeed when they speak the language of the business. Quantifying risk in financial terms, aligning with key stakeholders, and focusing on targeted, measurable actions will elevate security from a support function to a strategic driver of enterprise resilience.