Building and Scaling a Strategic Metrics Framework

This session explored how corporate security teams can build and mature data-driven metrics programs. Drawing on global research and practitioner insights, it highlighted key barriers including knowledge gaps, limited resources, and lack of leadership prioritization. Panelists emphasized practical approaches such as starting small, leveraging internal "data champions," improving data quality, and aligning analytics with executive decision-making to demonstrate value and drive adoption across enterprise security functions.

Speakers

Matt Alcoke
Associate Director, Threat Management and Investigations
Kirkland & Ellis

Ben Bissell
VP, Enterprise Security Data
BlackRock

Farhad Tajali
SVP, Global Head of Safety & Security
Creative Artists Agency

Key Themes and Topics

Closing the Security Analytics Knowledge Gap

Many security professionals lack foundational skills in data analysis, visualization, and tools, limiting program maturity. Addressing this gap through targeted training and internal capability building is critical to enabling meaningful insights and advancing beyond basic data collection toward strategic decision support.

The Role of Data Champions in Program Development

Organizations benefit from identifying or hiring "data-smart" individuals who understand both security operations and analytics. These individuals bridge strategic intent with execution, helping translate raw data into actionable insights and accelerating adoption without requiring full data science teams.

Leadership Buy-In as a Force Multiplier

Executive engagement, particularly through dashboards and recurring reporting, drives visibility and demand for analytics. When leaders actively use metrics in decision-making, it creates organizational momentum, encourages cross-team participation, and reinforces the value of data-driven security operations.

Continued on next page

Key Themes and Topics

Data Quality and Integrity as Foundational Requirements

Reliable analytics depend on structured, consistent data collection. Poor input quality undermines trust and limits usability. Standardized fields, reduced ambiguity, and controlled inputs improve accuracy, enabling executives to confidently rely on metrics for operational and strategic decisions.

Transitioning from Data Collection to Insight Generation

Most organizations collect data but fail to analyze or operationalize it. Mature programs integrate analytics into workflows, enabling continuous improvement, trend identification, and proactive decision-making. The shift from reporting to insight is essential for achieving measurable security outcomes.

Actionable Takeaways

Establish a Dedicated Data Champion

Identify or assign a security professional with both operational awareness and analytical aptitude to lead metrics development. This role should coordinate data efforts, align analytics with strategic priorities, and serve as the central driver of program maturity and adoption.

Mandate Regular Metrics Review Cadence

Implement monthly or quarterly security metrics reviews led by senior leadership. Requiring teams to present data ensures consistent engagement, reinforces accountability, and embeds analytics into operational rhythms and executive decision-making processes.

Standardize Data Collection Frameworks

Replace freeform inputs with structured fields, dropdowns, and defined taxonomies. This reduces ambiguity, improves data integrity, and ensures consistency across teams, enabling more accurate analysis and scalable reporting across the enterprise.

Start Small and Demonstrate Immediate Value

Begin with simple tools such as spreadsheets or basic dashboards to track key metrics. Quickly translate data into visual insights that resonate with leadership, building credibility and securing buy-in for further investment in analytics capabilities.

Continued on next page

Actionable Takeaways

Align Metrics with Executive Priorities

Focus data collection and reporting on risks and outcomes that matter most to leadership, such as executive threats, travel risk, or incident trends. Tailoring insights to business priorities increases relevance and drives sustained executive engagement.

Expand Data Integration Across Security Domains

Integrate data from multiple sources, including incident management, access control, intelligence, and travel systems. A unified view of risk enables deeper analysis, improves situational awareness, and supports more informed, enterprise-level decision-making.

Notable Quote

> **"Take the time to build something, even if it's just spreadsheets… and present it in the right way to get that buy-in and the realization that, oh, this is good stuff here. Then the resources will come."**

- Matt Alcoke
Associate Director, Threat Management and Investigations
Kirkland & Ellis

Final Message

Security metrics are no longer optional. Organizations that invest in structured data, leadership engagement, and practical analytics capabilities will move from reactive reporting to proactive risk management. Start with what you have, focus on data quality, and consistently demonstrate value to embed analytics at the core of your security strategy.