

Why Boards Need Cyber Risk Measured in Business Terms

November 2026 Webinar Backgrounder

Board-Level Metrics: Measuring Cyber Risk in Business Terms

2026 NACD–ISA Director’s Handbook on Cyber-Risk Oversight, Fifth Edition

Toolkit Focus: Tool K — Board-Level Cybersecurity Metrics

Background

Corporate boards routinely evaluate financial performance, operational resilience, investment effectiveness, and enterprise risk through measurable indicators. Cybersecurity presents a particular challenge: organizations generate extensive technical information, yet directors may still lack a clear understanding of how cyber threats translate into financial losses, business disruption, and strategic exposure.

Tool K, *Board-Level Cybersecurity Metrics*, authored by JR Williamson, Michael Higgins, and Nicola Sanna, addresses this challenge through five areas: the threat environment, economic loss exposure, cyber-risk profile, supply-chain exposure, and business and operational decisions (Williamson et al., 2026).

These categories reflect a fundamental governance problem: technical cybersecurity performance does not necessarily establish whether an organization's most consequential business risks are declining. This backgrounder examines why each of Tool K's five areas matters, drawing on independent research and documented incidents rather than repeating the toolkit's recommendations.

1. Tool K: What Is the Threat Environment We Face?

Tool K asks whether directors understand the threats facing their industry, the significance of recent incidents, and their potential consequences for business performance (Williamson et al., 2026).

This distinction matters because threat volume and business impact are not equivalent. Thousands of unsuccessful attacks may have limited consequences, while a single compromise of a critical system can disrupt essential operations.

Verizon's 2026 *Data Breach Investigations Report* examined more than 31,000 security incidents, including more than 22,000 confirmed breaches across 145 countries. The report documents the continuing importance of vulnerability exploitation, credential abuse, and third-party exposure in the threat landscape (Verizon, 2026).

These findings show why cybersecurity reporting must distinguish general threat activity from incidents that can materially affect the enterprise.

For directors, the issue is not simply how many attacks an organization experiences. It is whether management can identify threats most likely to disrupt critical operations, compromise sensitive information, or produce significant financial consequences.

Tool K's threat-environment category therefore addresses the need to translate cybersecurity intelligence into business-relevant risk information.

2. Tool K: What Is Our Cyber Loss Exposure in Economic Terms?

Tool K emphasizes understanding probable cyber-loss frequency, financial impact, critical assets, and exposure relative to enterprise risk appetite (Williamson et al., 2026).

The 2024 Change Healthcare cyberattack illustrates the importance of this perspective. UnitedHealth Group reported about \$2.2 billion in direct response costs in 2024, along with an estimated \$867 million in Optum Insight business-disruption impacts (UnitedHealth Group, 2025).

These amounts represent different financial effects and should not be treated as interchangeable. Together, they demonstrate that cyber incidents can create consequences extending beyond technical recovery.

Cyber incidents can affect revenue, operating costs, customer relationships, service availability, and organizational resilience. Technical recovery measures alone cannot adequately describe those consequences.

NIST's updated enterprise-risk guidance emphasizes connecting cybersecurity scenarios to likelihood, business impact, risk appetite, and organizational objectives (Quinn, Chua, et al., 2025; Quinn, Ivy, et al., 2025).

Although financial estimates involve uncertainty, expressing cyber exposure in economic terms lets directors compare cybersecurity risks with other enterprise exposures and assess whether risk acceptance aligns with financial objectives.

Tool K's emphasis on economic loss therefore connects cybersecurity oversight directly to the board's financial responsibilities.

3. Tool K: What Is Our Cyber-Risk Profile?

Tool K addresses cybersecurity maturity, control effectiveness, independent assessments, vulnerability exposure, and benchmarking against recognized frameworks (Williamson et al., 2026).

These measures matter because cybersecurity activity does not automatically reduce risk.

An organization may increase security spending, improve compliance scores, and remediate numerous vulnerabilities while remaining exposed through a critical application, weak identity controls, or an untested recovery process.

Similarly, vulnerability counts can misrepresent material exposure when individual weaknesses differ in exploitability, affected assets, and potential business consequences.

NIST's revised guidance on integrating cybersecurity and enterprise risk management emphasizes connecting cybersecurity assessments to organizational objectives and risk-management decisions (Quinn, Chua, et al., 2025).

The FAIR Institute's 2025 research also identifies business alignment, risk-based prioritization, and informed resource allocation as benefits associated with quantitative approaches to cybersecurity risk management (FAIR Institute, 2025).

These findings reinforce the distinction between measuring security work performed and evaluating whether that work reduces consequential business exposure.

For directors, the relevant issue is whether management's metrics provide credible evidence that the organization's material cyber-risk profile is improving, deteriorating, or remaining unchanged.

4. Tool K: What Is Our Supply-Chain Exposure?

Tool K addresses third-party dependencies, critical vendors, concentration risk, financial exposure, and operational resilience (Williamson et al., 2026).

The June 2024 cyberattack against CDK Global demonstrated why these issues matter. The disruption affected automobile dealerships that relied on CDK systems for essential business functions.

Sonic Automotive subsequently estimated that the outage adversely affected its 2024 reported income before taxes by approximately \$47.2 million (Sonic Automotive, 2025).

This amount represents an estimated adverse effect on reported pretax income, not a separately established direct cash loss.

The incident illustrates how a company can experience substantial financial consequences from an attack against an external technology provider, even when its own systems are not the original target.

Verizon's 2026 DBIR further identifies third-party involvement as a significant feature of the breach landscape (Verizon, 2026).

These findings demonstrate why internal cybersecurity metrics alone may provide an incomplete picture of enterprise exposure. A company may improve its own security posture while remaining dependent on external systems whose failure could interrupt revenue-generating operations.

Tool K's supply-chain category therefore reflects a central business reality: consequential cyber exposure can originate outside the organization's direct operational control.

5. Tool K: Are We Making the Right Business and Operational Decisions?

Tool K connects cybersecurity metrics to investment decisions, risk acceptance, insurance, strategic priorities, and the economic value of risk reduction (Williamson et al., 2026).

This category matters because cybersecurity resources are finite. Boards must evaluate security expenditures alongside competing investments in technology, operations, innovation, and growth.

The FAIR Institute's 2025 *State of Cyber Risk Management* research, based on a survey of 402 cyber-risk-management professionals, reported that nearly 45% of participating organizations were using or planning to use FAIR, while 90% of adopters reported successful implementation (FAIR Institute, 2025).

Because the survey focused on professionals already involved in cyber-risk management, these results should not be generalized to all organizations. They also do not establish that adopting a particular framework independently causes improved financial performance.

Nevertheless, the findings illustrate organizational interest in connecting cybersecurity analysis to business decisions.

Without credible estimates of exposure and expected risk reduction, management may struggle to explain why one cybersecurity investment deserves priority over another.

The same challenge applies to cyber insurance. Coverage decisions become more meaningful when directors understand plausible losses, retained risk, policy limitations, and the organization's capacity to absorb disruption.

Tool K's final category therefore connects cybersecurity measurement to capital allocation, risk tolerance, and enterprise value.

Concluding Observation

Tool K's five categories demonstrate why board-level cybersecurity metrics must extend beyond technical reporting.

Threat intelligence must establish business relevance. Economic analysis must clarify potential financial consequences. Cyber-risk profiles must indicate whether controls meaningfully reduce exposure. Supply-chain metrics must account for critical external dependencies. Investment measures must connect spending to risk reduction and enterprise value.

The documented financial effects of the Change Healthcare and CDK incidents, together with research from Verizon, NIST, and the FAIR Institute, reinforce the significance of these distinctions.

The governance challenge is not necessarily a shortage of cybersecurity data. It is converting that data into information directors can use to evaluate financial exposure, operational resilience, investment effectiveness, and management accountability.

The central question for the November webinar is: How can boards determine whether their organizations are managing cyber risk effectively when cybersecurity reporting does not clearly connect technical performance to business and financial outcomes?

References:

- FAIR Institute. (2025). *2025 state of cyber risk management report: From compliance to competitive advantage—The quantified value of cybersecurity*.
<https://www.fairinstitute.org/state-of-crm-2025>
- Quinn, S., Chua, J., Ivy, N., Gardner, R., Kent, K., Smith, M., & Witte, G. (2025). *Integrating cybersecurity and enterprise risk management (ERM)* (NIST IR 8286 Rev. 1). National Institute of Standards and Technology.
<https://doi.org/10.6028/NIST.IR.8286r1>
- Quinn, S., Ivy, N., Barrett, M., Feldman, L., Gardner, R., & Witte, G. (2025). *Identifying and estimating cybersecurity risk for enterprise risk management* (NIST IR 8286A Rev. 1). National Institute of Standards and Technology.
<https://doi.org/10.6028/NIST.IR.8286Ar1>
- Sonic Automotive, Inc. (2025). *Annual report for the fiscal year ended December 31, 2024*. <https://ir.sonicautomotive.com/sec-filings/annual-reports/content/0001043509-25-000003/sah-20241231.htm>
- UnitedHealth Group Incorporated. (2025). *Annual report for the fiscal year ended December 31, 2024*.
<https://www.sec.gov/Archives/edgar/data/731766/000073176625000063/unh-20241231.htm>

Verizon. (2026). *2026 data breach investigations report*.

<https://www.verizon.com/business/resources/reports/dbir/>

Williamson, J. R., Higgins, M., & Sanna, N. (2026, April 16). *Board-level*

cybersecurity metrics. National Association of Corporate Directors.

<https://www.nacdonline.org/all-governance/governance-resources/governance-research/director-handbooks/2026-cyber-risk-oversight/cyber-risk-handbook-toolkit-2026/board-level-cybersecurity-metrics/>