International Journal of Advanced Engineering and Management Research

Vol. 11, No. 02; 2026

ISSN: 2456-3676

Translating Cybersecurity Assessment Outputs for Board-level Oversight

Dr. Robb Shawe (Lead Author)
Dr. Gilbert B. Mengnjo (Co-Author)
Capitol Technology University, Department of Critical Infrastructure, 11301 Springfield Road, Laurel, MD 20708, USA

doi.org/10.51505/ijaemr.2026.11212 URL: http://dx.doi.org/10.51505/ijaemr.2026.11212

Received: Mar 06, 2026 Accepted: Mar 17, 2026 Online Published: Mar 24, 2026

Abstract
Boards of directors are increasingly held accountable for cybersecurity risk oversight across critical infrastructure sectors. In response, organizations routinely present cybersecurity assessment outputs—including maturity scores, dashboards, and compliance summaries—to support board decision-making. However, these materials often fail to provide boards with the clarity required to exercise effective oversight. The challenge is not a lack of information or excessive technical detail, but rather the absence of a structured translation that aligns assessment outputs with board responsibilities, risk appetite, and fiduciary duties. This qualitative, applied analysis examines how cybersecurity assessment outputs can be translated into governance-relevant narratives that support meaningful board-level oversight without oversimplifying risk. Drawing on risk communication, governance, and information-asymmetry perspectives, the article explains why current reporting practices underperform and proposes a translation-focused governance approach that links technical assessment results to accountability, prioritization, and executive action. The study contributes a board-centric framework to improve oversight effectiveness and reduce systemic cyber risk in critical infrastructure organizations.

Keywords: Board oversight; cybersecurity governance; risk communication; assessment translation; fiduciary responsibility; critical infrastructure; executive accountability

1. Introduction

This article advances the argument that cybersecurity assessment outputs must be translated into governance-aligned risk narratives to enable effective board-level oversight. Cybersecurity has evolved into a core governance responsibility for boards of directors, particularly within critical infrastructure sectors such as healthcare and energy, where digital disruption carries operational, safety, and regulatory consequences (Cybersecurity and Infrastructure Security Agency [CISA], 2024; U.S. Department of Energy [DOE], 2022). Regulators, investors, and courts increasingly expect boards to demonstrate informed oversight of cyber risk rather than reliance on management assurances alone (National Association of Corporate Directors [NACD], 2023; Securities and Exchange Commission [SEC], 2023a).

Vol. 11, No. 02; 2026

ISSN: 2456-3676

To support board oversight, organizations routinely rely on cybersecurity assessments and maturity models to generate structured information. Assessment outputs—often presented as maturity scores, dashboards, or heat maps—are intended to provide boards with visibility into organizational cyber posture. Despite their prevalence, these outputs frequently fail to support meaningful board-level decision-making (National Institute of Standards and Technology [NIST], 2024).

This disconnect is often mischaracterized as a need to simplify technical information for non-technical audiences. In practice, oversimplification can exacerbate governance risk by obscuring uncertainty, dependencies, and accountability. The core challenge is not simplification but **governance reframing**: aligning assessment outputs with board authority, fiduciary duty, and risk-acceptance decisions. It argues that without structured translation, assessments risk becoming symbolic artifacts that convey activity rather than actionable insight, leaving boards exposed despite abundant information.

This manuscript constitutes a segment of an extensive research initiative aimed at examining the interpretation of cybersecurity governance within critical infrastructure sectors. The series explores how cybersecurity evaluations, maturity models, and governance frameworks affect organizational learning, risk-management prioritization, and resilience in intricate socio-technical systems. By merging interdisciplinary academic analysis with insights derived from practitioners, the research endeavors to elucidate how governance structures, regulatory environments, and organizational accountability influence the efficacy of cybersecurity risk mitigation and operational resilience.

1.1 Methodological Orientation

This study adopts a qualitative, applied governance analysis examining how cybersecurity assessment outputs are translated into board-level narratives. Drawing on the contexts of healthcare and energy infrastructure, the analysis evaluates the transformation of technical maturity outputs into executive risk-communication frameworks. The focus is not on technical control validation but on governance-level interpretive processes, information asymmetry, and the efficacy of oversight. The approach is conceptual and translational rather than empirical.

The analytical approach applies a comparative governance lens to examine how cybersecurity assessment outputs are interpreted across different critical infrastructure contexts. The study evaluates how technical findings are translated into governance-relevant narratives and how these interpretations influence the effectiveness of oversight, accountability structures, and decision-making processes. Rather than testing hypotheses empirically, the analysis synthesizes theoretical frameworks and sector-specific practices to construct a conceptual model of assessment translation and its impact on governance.

Vol. 11, No. 02; 2026

ISSN: 2456-3676

2. Background and Context

2.1 Board-level cybersecurity governance

Board oversight of cybersecurity has expanded significantly in recent years. Governance literature emphasizes that boards are responsible for risk oversight, strategic alignment, and executive accountability rather than operational control.

In this article, the term cybersecurity assessment outputs refers to the structured findings generated by standardized cybersecurity assessment instruments.

In cybersecurity contexts, this responsibility requires boards to understand material risk exposure, approve risk tolerance, and ensure that management actions align with organizational objectives (NACD, 2023; SEC, 2023a).

Boards typically lack deep technical expertise and therefore depend on management-provided information to fulfill these duties. This dependency heightens the importance of how cybersecurity information is framed and communicated.

2.2 Current practices in cyber risk reporting

Cyber risk reporting to boards commonly relies on maturity scores, traffic-light dashboards, compliance summaries, and aggregated metrics derived from assessment tools. While efficient, these formats often prioritize status over consequences and obscure the relationship between assessment results and enterprise risk, operational resilience, and accountability (Boyens et al., 2022; Stine et al., 2020).

2.3 Limitations of technical metrics for governance audiences

Technical assessment outputs are designed to evaluate control implementation, not to support fiduciary decision-making. Metrics optimized for practitioners may lack contextual framing necessary for board interpretation, leading to false assurance, misaligned priorities, or decision paralysis (NIST, 2024). Without translation, boards may receive extensive data yet remain unable to act effectively.

In practice, organizations frequently conduct recurring cybersecurity assessments that generate detailed findings but fail to produce corresponding governance actions. For example, healthcare organizations may repeatedly identify vulnerabilities in clinical system access controls, while energy providers may document persistent weaknesses in operational technology segmentation. Despite these findings, remediation efforts may be delayed due to competing priorities, unclear ownership, or insufficient escalation of governance. This pattern illustrates how assessment fatigue can emerge, where repeated evaluation does not translate into meaningful risk reduction, reinforcing the need for governance structures that prioritize action over assessment volume.

Vol. 11, No. 02; 2026

ISSN: 2456-3676

2.4 Gap in existing approaches

Despite widespread assessment activity, limited guidance exists on **aligning cybersecurity assessment outputs with board-relevant governance narratives**. This gap contributes to persistent misalignment between technical reporting and oversight responsibilities, particularly in complex, critical-infrastructure organizations. This analysis forms part of a broader, multi-article research program examining the governance and interpretation of cybersecurity assessment outputs across critical infrastructure contexts (Shawe, 2026).

3. Problem Statement

It is not known how cybersecurity assessment outputs can be effectively translated to support meaningful board-level oversight without oversimplifying risk.

As a result, boards may receive abundant cybersecurity information yet lack the clarity necessary to make informed decisions regarding risk acceptance, investment prioritization, and executive accountability.

4. Purpose of the Study

The purpose of this qualitative, applied analysis is to examine how cybersecurity assessment outputs can be translated into board-level governance narratives across critical infrastructure sectors.

The study focuses on the translation and use of existing assessment outputs rather than the development of new tools, emphasizing governance relevance, decision support, and accountability.

5. Research Questions

RQ1: What cybersecurity information do boards require to exercise effective oversight?

RQ2: How are cybersecurity assessment outputs currently communicated to boards?

RQ3: What translation strategies improve board understanding, accountability, and decision-making?

6. Theoretical and Conceptual Framework

This study integrates three complementary theoretical perspectives.

Risk communication theory emphasizes audience-specific framing and relevance. Information is practical only when it supports the decisions the audience is empowered to make.

Vol. 11, No. 02; 2026

ISSN: 2456-3676

Governance and oversight theory defines the board's role in setting risk appetite, overseeing management, and ensuring accountability rather than engaging in operational detail (NACD, 2023).

Information asymmetry and decision-making theory explain how disparities in expertise between technical professionals and boards distort interpretation, even when data is plentiful (Stine et al., 2020).

Together, these perspectives support a framework in which cybersecurity assessment outputs must be translated—not simplified—to align risk meaning with board authority.

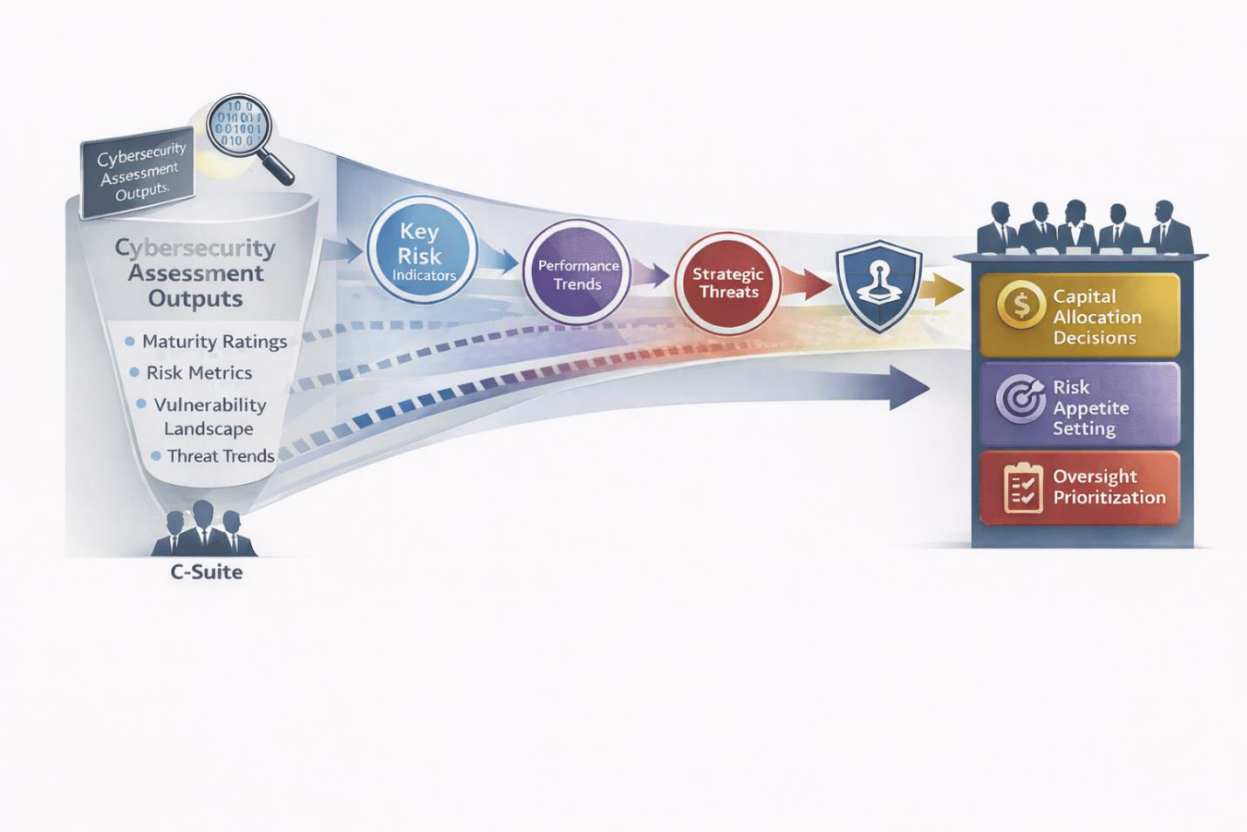
Figure 1 illustrates the governance-aligned translation pathway through which cybersecurity assessment outputs are transformed into board-relevant risk narratives that support oversight, accountability, and decision-making.

Vol. 11, No. 02; 2026

ISSN: 2456-3676

Figure 1

Translation Pathway from Cybersecurity Assessment Outputs to Board-Level Risk Oversight



Note. Author created. The figure illustrates a conceptual translation pathway that transforms detailed cybersecurity assessment outputs—such as maturity ratings, risk metrics, vulnerability landscape data, and threat trends—into governance-relevant risk narratives. The model filters technical findings into key risk indicators, performance trends, and strategic threat assessments that inform board-level decisions on capital allocation, risk appetite setting, and oversight prioritization. The framework is conceptual and intended to depict governance communication and fiduciary oversight dynamics rather than to measure board behavior or decision outcomes.

Figure 1 depicts the governance translation architecture through which technical cybersecurity findings are transformed into board-level risk indicators that guide decisions on capital allocation, risk appetite, and oversight prioritization. The model distinguishes between information presentation and decision-enabling translation, emphasizing that effective governance depends on aligning assessment outputs with board authority and accountability structures. Taken together, this framework demonstrates that the effectiveness of cybersecurity assessment at the board level depends on the alignment of technical findings with governance authority, fiduciary responsibility, and decision accountability.

Vol. 11, No. 02; 2026

ISSN: 2456-3676

7. Significance of the Study

This study advances cybersecurity governance by shifting attention from assessment generation to assessment utilization. It explains why boards may be unable to exercise effective oversight despite receiving regular cybersecurity reports.

For organizations, the analysis supports improved board engagement and accountability. For regulators and stakeholders, it reinforces the importance of governance-aligned reporting in meeting fiduciary and duty-of-care expectations (SEC, 2023a; NIST, 2024).

8. Organization of the Article

The article reviews board-level cybersecurity governance challenges, examines limitations of current reporting practices, develops a translation-focused governance approach, and discusses implications for oversight and accountability.

9. Translating Assessment Outputs for Board Oversight

Effective governance-oriented framing aligns assessment outputs with board decision domains. Rather than reporting control status alone, translated narratives should address three governance questions: **What risk exists? Who is accountable? What decision is required?**

Assessment results should be contextualized in terms of business impact, interdependencies, and alignment with the stated risk appetite. This approach enables boards to engage meaningfully without requiring technical immersion (Stine et al., 2020; Mengnjo, 2026).

Table 1 illustrates how governance conditions shape whether cybersecurity assessment outputs translate into actionable outcomes or persist as recurring findings without remediation across critical infrastructure contexts.

Vol. 11, No. 02; 2026

ISSN: 2456-3676

Table 1

Comparative Interpretation of Cybersecurity Controls Across Critical Infrastructure Sectors

Governance Condition	Assessment Outcome
Clear remediation ownership	Assessment findings trigger corrective action.
Integration with enterprise risk governance	Assessment results inform strategic decision-making.
Accountability mechanisms for remediation	Repeated findings decline over time.
Diffuse responsibility for findings	Findings recur across assessments.
Symbolic compliance culture	Assessments become performative exercises rather than drivers of improvement.

Note. Author created. The table illustrates how identical cybersecurity controls are interpreted differently across critical infrastructure sectors based on mission-critical priorities and operational risk contexts.

Collectively, these governance conditions demonstrate that the value of cybersecurity assessment is determined not by the identification of findings alone, but by the presence of governance structures that translate those findings into accountable action and measurable risk reduction.

10. Assessment-to-Action Pathways in Cybersecurity Governance

Cybersecurity assessment outputs may follow divergent governance pathways depending on how findings are interpreted and acted upon. In failure pathways, assessment results are archived, deprioritized, or disconnected from resource allocation and executive accountability, leading to recurring vulnerabilities and the normalization of unresolved risk. In contrast, resilience pathways translate assessment findings into governance actions, including budget allocation, ownership assignment, and performance tracking tied to executive accountability. This distinction highlights that the value of cybersecurity assessments is not determined by the volume of findings generated but by the extent to which those findings influence decision-making, resource prioritization, and organizational behavior. Effective governance, therefore, requires structured mechanisms that convert assessment outputs into actionable outcomes rather than symbolic compliance artifacts.

Vol. 11, No. 02; 2026

ISSN: 2456-3676

In this context, assessment fatigue should be understood not as an operational inefficiency but as a systemic governance failure.

11. Implications for Governance and Practice

Organizations should redesign cybersecurity reporting processes to emphasize **decision-aligned communication** over summarization. This includes mapping assessment findings to enterprise risks, clarifying ownership of deficiencies, and explicitly linking results to executive and board-level decisions (COSO, 2017; Quinn, 2025).

Boards benefit when assessment outputs are framed as governance inputs rather than technical artifacts. Such translation strengthens oversight, improves accountability, and reduces the likelihood of governance-level cyber failures (Boyens et al., 2022; Shawe, 2026).

12. Limitations and Future Research

This study advances a qualitative, governance-oriented framework for translating cybersecurity assessment outputs into board-level oversight narratives. The analysis is conceptual and applied in nature and does not evaluate specific board deliberations, measure director comprehension, or empirically assess decision outcomes resulting from assessment translation. While healthcare and energy infrastructure contexts provide sectoral grounding, the framework is not statistically generalizable across all critical infrastructure sectors without contextual adaptation.

Additionally, the study does not test the proposed translation model through experimental or observational methods involving board members. Instead, it synthesizes established governance theory, risk-communication scholarship, and documented sector practices to refine an interpretive pathway from technical-maturity outputs to fiduciary-oversight decisions. The proposed framework should therefore be understood as a governance-analytic model rather than as an empirically validated predictor of board behavior.

Future research may extend this work through structured interviews with board members, comparative analysis of board-level cybersecurity reporting practices, or case studies examining how assessment translation influences capital allocation, risk prioritization, and oversight efficacy. Empirical validation across additional sectors may further clarify how governance context, regulatory environment, and board composition influence the effectiveness of cybersecurity assessment translation strategies.

13. Conclusion

Cybersecurity assessments generate extensive information, yet board-level cyber failures persist. This paradox reflects a failure of translation rather than measurement. Translating assessment outputs into governance-relevant narratives enables boards to fulfill their oversight responsibilities without oversimplifying risk. In critical infrastructure organizations, effective

Vol. 11, No. 02; 2026

ISSN: 2456-3676

translation is essential to align cybersecurity practices with fiduciary accountability and organizational resilience.

Authorship Statement

Dr. Robb Shawe and Dr. Gilbert Mengnjo jointly conceptualized the research orientation and governance perspective of this manuscript. Dr. Mengnjo contributed practitioner expertise spanning more than 15 years in cybersecurity governance, enterprise risk management, regulatory compliance, and healthcare information security.

Dr. Shawe contributed a multidisciplinary scholarly synthesis integrating critical infrastructure protection, cybersecurity governance, organizational resilience, and socio-technical systems theory. Dr. Shawe also led the development of the conceptual framing, the integration of the literature, and the preparation of the manuscript.
Both authors collaborated in refining the analytical framework, reviewing the manuscript, and approving the final version for submission.

This manuscript forms part of a broader **scholarly program of research** examining cybersecurity governance, risk management maturity, and resilience across critical infrastructure and organizational ecosystems.

Author Note and Copyright Statement

Dr. Robb Shawe, PhD, MS

Dr. Robb Shawe is a scholar-practitioner, U.S. Navy veteran, and Chief Executive Officer of New York Security Consulting Professionals L.L.C. His research focuses on critical infrastructure protection, cybersecurity governance, organizational resilience, and socio-technical risk management. His scholarship integrates multidisciplinary perspectives spanning cybersecurity, emergency management, occupational health, and sustainability systems.

Dr. Shawe served as the lead author and was primarily responsible for conceptualization, development of the analytical framework, literature synthesis, and manuscript preparation. His work emphasizes the integration of governance structures, resilience systems, and policy frameworks designed to strengthen critical infrastructure and organizational security environments.

Dr. Gilbert Mengnjo, PhD, MSc

Dr. Gilbert Mengnjo is a cybersecurity governance strategist and risk management leader with more than 15 years of experience guiding enterprise cybersecurity programs across healthcare, manufacturing, global supply chains, and critical infrastructure environments. His expertise includes cybersecurity governance, regulatory compliance, vendor risk management, and

Vol. 11, No. 02; 2026

ISSN: 2456-3676

security program development aligned with frameworks such as NIST CSF, HIPAA, HITRUST, and ISO 27001.

Dr. Mengnjo contributed practitioner insights, governance analysis, and applied cybersecurity expertise to the conceptual development of the research framework and literature synthesis. His experience translating complex technical risks into operational governance strategies informed the manuscript's analytical perspective.

Conflict of Interest Statement

The authors declare no conflicts of interest related to this research.

Originality Statement

This manuscript represents original scholarly work and is not currently under consideration by another publication outlet.

Copyright Notice

References

Boyens, J. M., Paulsen, C., Bartol, N., Winkler, K., & Gabel, O. (2022). *Cybersecurity supply chain risk management practices for systems and organizations* (NIST SP 800-161 Rev. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-161r1

Committee of Sponsoring Organizations of the Treadway Commission. (2017). *Enterprise risk management—Integrating with strategy and performance*. https://www.coso.org

Cybersecurity and Infrastructure Security Agency. (2024). *Cyber Security Evaluation Tool (CSET®)*. https://www.cisa.gov/cset

Mengnjo, G. B. (2026). *Assessing healthcare supply chain cybersecurity using the Cyber Security Evaluation Tool (CSET®) (Unpublished doctoral dissertation)*. Capitol Technology University.

National Association of Corporate Directors. (2023). *Director's handbook on cyber-risk oversight* (4th ed.). https://www.nacdonline.org

National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0*. https://www.nist.gov/cyberframework

Quinn, S. (2025). *Integrating cybersecurity and enterprise risk management (ERM)* (NISTIR 8286 Rev. 1). National Institute of Standards and Technology. https://csrc.nist.gov

Vol. 11, No. 02; 2026

ISSN: 2456-3676

Securities and Exchange Commission. (2023a). *Cybersecurity risk management, strategy, governance, and incident disclosure* (Final rule). https://www.sec.gov

Shawe, R. (2025). *Exploring smart grid technologies' impact on sustainable energy management in New York State* (Publication No. 32284053) [Doctoral dissertation, Capitol Technology University]. ProQuest Dissertations & Theses Global.

Stine, K., Quinn, S., Witte, G., Gardner, R., & Lorenzen, D. (2020). *Integrating cybersecurity and enterprise risk management (ERM)* (NISTIR 8286). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8286

U.S. Department of Energy. (2022). *Cybersecurity Capability Maturity Model (C2M2), Version 2.1*. https://www.energy.gov