WHITE PAPER

From Operational Security to Fiduciary Oversight

Reframing Cyber Risk Governance for the Enterprise

Publication Code	PD-WP-001
Version	1.0
Published	July 2026
Category	Cyber Risk Governance & Accountability™ (CRGA™)
Issued By	Praesidium Governance, Inc.
Canonical URL	praesidiumoversight.com/publications/white-papers/from-operational-security-to-fiduciary-oversight/
PDF Download	praesidiumoversight.com/publications/white-papers/PD-WP-001_From_Operational_Security_to_Fiduciary_Oversight_v1_0.pdf

Document Status	Analytical Publication
Authority Level	Institutional
Applicability	Cyber Risk Governance & Accountability™
Supersession	This document may be revised by subsequent Praesidium publications.

LEGAL NOTICE AND TERMS OF USE

COPYRIGHT

TRADEMARK NOTICE

PERMITTED USE

This publication may be distributed in its complete and unaltered form for non-commercial informational purposes only. Any reproduction, excerpting, or reference must preserve full attribution to Praesidium Governance, Inc. and may not alter the meaning, context, or presentation of Praesidium's institutional position, including through partial or selective excerpting.

PROHIBITED USE

Reproduction for commercial purposes, redistribution for compensation, modification or creation of derivative works, removal of attribution or copyright notices, and use in any manner that misrepresents the source, authorship, or institutional position of this content are strictly prohibited.

NO CERTIFICATION, ASSURANCE, OR ATTESTATION

This publication does not constitute and shall not be construed as a certification, accreditation, assurance engagement, attestation, audit opinion, or warranty of any kind regarding any organization, product, service, control environment, or governance arrangement. Praesidium Governance, Inc. does not issue certifications or accreditations and makes no representations that any organization or individual is certified, accredited, approved, or endorsed under the CRGA™ framework or any Praesidium publication.

NO ADVISORY RELATIONSHIP

This publication is provided for governance education, institutional review, and category-architecture reference only. It does not constitute legal, regulatory, financial, technical, operational, or compliance advice. No advisory, consulting, fiduciary, or professional services relationship is assumed or created by the issuance or receipt of this publication. Recipients should consult qualified independent professionals for advice specific to their circumstances.

NO ENDORSEMENT

Reference to CRGA™, alignment with its principles, or citation of Praesidium publications does not constitute endorsement, approval, certification, validation, or affiliation with Praesidium Governance, Inc.

STRUCTURAL INDEPENDENCE

Praesidium Governance, Inc. is an independent governance architecture authority and category steward. It does not provide operational cybersecurity services, managed security services, compliance audits, technology implementation, or vendor-affiliated advisory services. This structural independence is a design condition of Praesidium's authority as category steward of CRGA™. No commercial relationship with any vendor, insurer, regulator, or service provider affects the content of Praesidium publications.

LIMITATION OF LIABILITY

To the fullest extent permitted by applicable law, Praesidium Governance, Inc. shall not be liable for any direct, indirect, incidental, consequential, special, or exemplary damages arising from or related to the use of, reliance on, inability to use, or misapplication of this publication or any content herein.

ACCURACY AND UPDATES

Praesidium Governance, Inc. makes no representations or warranties, express or implied, regarding the completeness, accuracy, currency, or applicability of the information contained herein, including without limitation any implied warranties of merchantability or fitness for a particular purpose. The content reflects Praesidium's institutional positions as of the publication date and may be revised or superseded by subsequent publications. Readers are responsible for verifying currency against the canonical publication record at praesidiumoversight.com.

GOVERNING AUTHORITY AND CONTACT

This publication is issued under the authority of Praesidium Governance, Inc., the independent governance architecture authority and category steward for Cyber Risk Governance & Accountability™ (CRGA™). The canonical version of this publication is maintained at praesidiumoversight.com. Questions regarding permitted use, licensing, or the CRGA™ framework should be directed to Praesidium Governance, Inc. through praesidiumoversight.com. The full Legal Notice, Terms of Use, and Disclosures governing use of Praesidium publications and the praesidiumoversight.com website are available at praesidiumoversight.com/legal/.

EXECUTIVE SUMMARY

Cyber risk has outgrown the operational frame through which many institutions still manage it.

For years, cyber risk was treated primarily as a security, technology, compliance, or incident-response matter. That treatment was understandable. Cyber risk emerged from technical systems, was managed by technical teams, and was measured through controls, alerts, vulnerabilities, maturity models, frameworks, assessments, and response capability.

Those tools remain necessary. They are no longer sufficient.

Cyber risk now affects enterprise value, regulatory exposure, customer trust, operational resilience, insurance posture, contractual obligations, disclosure expectations, third-party reliance, public statements, and board accountability. When a risk operates at that level, the relevant question is no longer only whether the institution has a cybersecurity program. The question is whether the institution can demonstrate that cyber risk was governed.

That requires a different architecture.

External board guidance is converging around the same institutional reality. The 2026 NACD/ISA Director's Handbook on Cyber-Risk Oversight reinforces that cyber risk is now a board-level oversight matter, not merely an operational technology issue. That convergence is important, but it does not by itself solve the governance problem. Board guidance may establish the expectation that directors oversee cyber risk. The institutional question remains whether the organization has built the governance architecture required to make that oversight exercisable, accountable, and defensible.

Operational security asks whether the institution has the controls, capabilities, personnel, tools, and response mechanisms required to manage cyber threats. Fiduciary oversight asks whether the institution has defined who has authority over cyber risk decisions, when escalation is mandatory, who is accountable, how oversight is evidenced, and whether the governance structure can withstand scrutiny after a consequential event.

This white paper argues that cyber risk governance must be reframed from an operational security function into an enterprise governance architecture. That shift does not require boards to manage cybersecurity operations. It requires institutions to define the structure through which cyber risk becomes a governed enterprise decision.

That is the function of CRGA™ Governance Architecture.

CORE THESIS

The shift from operational security to fiduciary oversight is not a technology change.

It is a governance architecture change.

An institution can have a mature cybersecurity program and still lack a defensible governance structure for cyber risk. It can have tools, policies, dashboards, incident response plans, controls, vendors, committees, assessments, and reports while still being unable to demonstrate who had authority, when escalation was required, who was accountable, what evidence showed oversight, and whether the board was engaged at the right level and at the right time.

Those are not merely operational questions.

They are governance questions.

They are the questions that arise when cyber risk becomes material to the institution, when an incident becomes a board matter, when a regulatory inquiry tests the record, when an insurer challenges representations, when a customer asks what governance existed, or when directors are asked to explain how oversight occurred.

Cyber risk governance therefore cannot be satisfied by operational security maturity alone. It requires an institutional structure capable of connecting cyber risk activity to fiduciary oversight, enterprise accountability, and defensible evidence.

I. The Limits of the Operational Security Frame

Cybersecurity programs are usually built around operational needs. They identify assets, assess threats, deploy controls, monitor systems, manage vulnerabilities, respond to incidents, engage vendors, support compliance, and report on program maturity. These activities are necessary. No serious cyber governance model can function without operational capability beneath it.

But operational capability is not the same as governance.

The operational security frame tends to ask whether controls are in place, whether vulnerabilities are being remediated, whether incidents are being detected, whether policies are being followed, whether frameworks are being mapped, whether tools are performing, and whether risks are being reported. These are important questions. They are not the full governance question.

A control can exist without a defined owner of the enterprise decision behind it. A dashboard can report risk without defining when escalation is mandatory. A framework can organize activity without assigning authority. A committee can meet without clarifying decision rights. A policy can describe expectations without producing oversight evidence. A vendor can support execution without creating institutional accountability.

This is the central limitation of the operational security frame: it manages activity, but it does not necessarily define authority.

That distinction matters because cyber risk now routinely moves beyond the operational environment in which it first appears. A vulnerability can become a customer trust issue. A third-party incident can become a contractual or insurance issue. An intrusion can become a disclosure issue. A ransomware event can become a board oversight issue. A control failure can become an enforcement issue. A delayed escalation can become a governance failure.

When cyber risk crosses that threshold, the institution is no longer being judged only by whether the technical program worked. It is being judged by whether the institution can demonstrate how the risk was governed.

II. Why Cyber Risk Has Become an Enterprise Governance Issue

Cyber risk has become enterprise governance risk because cyber events increasingly produce consequences that extend beyond the security function. They may affect revenue, operations, legal exposure, regulatory posture, customer trust, insurance recovery, investor confidence, board oversight, and executive accountability.

This does not mean every cyber issue belongs on the board agenda. It means the institution must define which cyber issues become governance issues and why.

That is where many organizations remain underdeveloped. They have severity ratings, but not governance materiality thresholds. They have incident response plans, but not decision-rights architecture. They have dashboards, but not escalation discipline. They have policies, but not accountability architecture. They have activity records, but not always oversight evidence. They have vendors, advisors, and internal teams, but not always structural independence between execution, reporting, validation, and governance authority.

The result is a predictable institutional gap.

The organization may be operationally active but governance-fragile. It may know what happened but struggle to show how decisions were governed. It may have records but lack defensible evidence that authority was defined, escalation was required, accountability was assigned, and oversight occurred before the institution was forced to explain itself.

This gap often remains hidden during ordinary operations. It becomes visible under pressure.

That pressure may come from a regulator, insurer, customer, investor, auditor, board committee, litigation process, public disclosure obligation, or internal post-event review. When it arrives, the institution may discover that it has a cybersecurity record but not a governance record.

That is the difference between managing cyber activity and governing cyber risk.

III. External Board Guidance Is Converging on the Same Point

External board guidance increasingly reflects the same underlying shift: cyber risk is no longer adequately understood as a technical issue delegated to operational teams. It is a board-level governance issue tied to enterprise value, fiduciary oversight, disclosure, resilience, and accountability.

The 2026 NACD/ISA Director's Handbook on Cyber-Risk Oversight is a useful example of that convergence. NACD describes the fifth edition as a board-focused resource built around cyber-risk oversight principles and practical tools for directors. The handbook reflects the broader market movement away from cyber as a narrow technology issue and toward cyber as an enterprise governance issue.

That convergence matters because it confirms the oversight expectation.

But oversight expectation alone does not create governance architecture.

The distinction is critical. Board guidance can establish that directors should oversee cyber risk. It can clarify that cyber risk belongs within the board's oversight responsibilities. It can encourage directors to engage management, assess preparedness, evaluate reporting, and understand the governance implications of cyber risk.

Praesidium's role is different.

Praesidium defines the governance architecture required to make that oversight exercisable, accountable, and defensible.

In CRGA™ terms, cyber-risk oversight requires more than board awareness, reporting cadence, or technical briefing quality. It requires defined decision rights, escalation discipline, accountability architecture, structural independence, stable governance language, and oversight evidence. Without those conditions, a board may receive more information without gaining a defensible governance structure.

This distinction preserves the proper relationship between external board guidance and Praesidium's category architecture. NACD/ISA guidance can validate that cyber risk has become a board-level oversight issue. Praesidium's CRGA™ Governance Architecture defines how institutions structure authority, escalation, accountability, and evidence so that oversight can be demonstrated when decisions are later questioned.

The implication is not that Praesidium should restate, reproduce, or repackage external board guidance. The implication is that external board guidance strengthens the need for Praesidium's original contribution: a governance architecture that sits above operational security and makes cyber-risk oversight institutionally governable.

IV. The Board Does Not Need to Operate Cybersecurity

A common objection to board-level cyber governance is that directors should not be expected to manage technical operations.

That objection is correct.

Boards should not operate the cybersecurity program. They should not select every tool, approve every technical control, review every vulnerability, manage incident response teams, or substitute their judgment for specialized operational expertise.

External board guidance has increasingly reinforced the importance of director engagement in cyber-risk oversight. But director engagement does not mean operational substitution. The governance question is not whether the board can perform the work of cybersecurity management. The governance question is whether the institution has defined the structure through which cyber risk becomes an enterprise decision.

The board-level responsibility is not to operate cybersecurity. It is to ensure that cyber risk is governed when it becomes material to the institution. That requires clarity around which cyber decisions are delegated to management, which decisions are retained by executive leadership, which conditions require board awareness, which matters require board action or review, who is accountable for consequential cyber decisions, and what evidence demonstrates that oversight occurred.

The board does not need to manage the control environment. It does need to know whether the institution has a governance architecture around the control environment.

This is the central distinction.

Operational teams manage cyber activity. Boards oversee the governance structure through which cyber risk becomes an institutional decision.

Without that structure, board reporting can become a substitute for board governance. Directors may receive information, but the institution may not have defined what that information requires. Management may report regularly, but escalation thresholds may remain informal. Security teams may maintain dashboards, but the dashboard may not be connected to authority, accountability, or board-relevant decision-making.

Being informed is not the same thing as governing.

V. Decision Rights: The First Governance Question

The first requirement of fiduciary oversight is decision-rights clarity.

Cyber risk governance fails when consequential decisions are made without a defined authority structure. This can occur even in capable organizations. Security may identify the risk. Technology may manage the environment. Legal may evaluate obligations. Risk may classify exposure. Finance may assess cost. Communications may prepare stakeholder messaging. Executive leadership may weigh enterprise consequences. The board may later ask whether it should have been informed sooner.

Each function may be acting reasonably within its own domain. Yet the institution may still lack clarity about who had authority over the consequential decision.

That is the governance issue.

Cyber risk decisions often involve tradeoffs that exceed technical judgment. Whether to delay remediation, accept residual risk, approve a compensating control, continue operating a vulnerable system, classify an incident as material, notify customers, involve the insurer, or escalate to the board may require technical input, legal judgment, business judgment, financial analysis, reputational assessment, and executive authority.

The governance question is not whether those perspectives were present. It is whether the institution defined who had authority to decide.

If authority is undefined, accountability becomes difficult to assign after the fact. The organization may be able to show that many people were involved, but involvement is not the same as authority. Participation does not prove decision rights. Consultation does not establish accountability.

Fiduciary oversight requires the institution to define who can decide, who can defer, who can escalate, who can accept risk, and who must be informed when cyber risk becomes consequential.

That structure should exist before the event.

VI. Escalation Discipline: When Information Must Move

The second requirement is escalation discipline.

Cyber governance often fails not because information was unavailable, but because the institution had not defined when information must move from one level of authority to another.

Escalation cannot depend entirely on informal judgment. If escalation is discretionary, the institution may struggle to explain why an issue reached leadership when it did, why it did not reach the board earlier, or why a particular risk was treated as operational until external pressure made it institutional.

This is especially important because cyber information is often abundant. Many institutions have alerts, severity labels, incident records, vulnerability scores, risk registers, control ratings, maturity assessments, dashboard indicators, and third-party reports. The problem is not always absence of information. The problem is that the information is not always tied to governance thresholds.

A dashboard may show an issue, but it does not define whether escalation is mandatory. An incident response plan may describe workflow, but it may not define governance materiality. A risk register may capture a condition, but it may not establish whether executive or board attention is required. A technical severity score may support triage, but it is not the same as an institutional consequence threshold.

Escalation discipline turns cyber information into governance action.

It defines the conditions under which cyber risk must move upward. Those conditions may involve material business impact, customer harm, regulatory exposure, insurance implications, third-party dependency, operational disruption, reputational exposure, potential disclosure relevance, board-level policy implications, repeated control failure, or failure to meet prior remediation commitments.

Without escalation discipline, reporting may increase visibility while leaving governance undefined.

That is not a reporting problem.

It is a governance architecture problem.

VII. Accountability Architecture: More Than a Responsible Name

The third requirement is accountability architecture.

Accountability is often reduced to naming a responsible person, role, function, committee, or owner. That may be necessary, but it is not sufficient. A name in a RACI, policy, committee charter, board deck, risk register, or operating model does not itself create accountability architecture.

Accountability architecture defines how responsibility is assigned, how authority is exercised, how escalation occurs, what evidence must be maintained, and how accountability can be evaluated when decisions are later examined.

This matters because cyber risk is rarely owned by one function alone. It often involves security, technology, legal, risk, finance, operations, communications, procurement, vendors, executives, and the board. Shared responsibility may support effective operations, but it can also obscure accountability.

When many parties are involved, the institution may later be able to describe participation but not ownership. It may know who attended the meeting, who received the dashboard, who commented on the risk, or who was copied on the incident update. But those facts do not necessarily show who was accountable for the decision.

Fiduciary oversight requires more than participation records. It requires evidence that accountability was assigned before the outcome was known.

This is where operational security and governance architecture separate. Operational security may show what the organization did. Accountability architecture shows who had authority, who was responsible, when escalation was required, how decisions were governed, and what evidence demonstrates that oversight occurred.

Without accountability architecture, cyber risk may be actively managed but institutionally ambiguous.

That ambiguity becomes dangerous when decisions are questioned.

VIII. Structural Independence: Whether Accountability Can Be Evaluated

The fourth requirement is structural independence.

Cyber risk governance depends on information from management, technical teams, advisors, vendors, auditors, and execution partners. That reliance is unavoidable. Boards and executives cannot govern without information from those closest to the work.

But when the same structure defines the expectation, executes the work, reports on performance, and validates the result, governance can become self-referential.

This creates false assurance.

The institution may have reports, dashboards, assessments, committee updates, maturity scores, remediation plans, and documentation. The record may appear thorough. The work may even be competent. But the governance question remains: was accountability capable of being evaluated independently, or was the institution relying on the same structure to perform, report, and validate its own adequacy?

This is not primarily a trust issue. It is a design issue.

Strong operators still need independent governance architecture. Excellent execution does not eliminate the need for separation between authority, execution, reporting, and validation. In fact, the stronger the execution environment becomes, the more important it is to preserve clarity about which party is performing the work, which party is governing the standard, which party is validating the result, and which party is accountable for the institutional decision.

Structural independence matters because oversight must remain capable of challenging the narrative it receives.

When accountability can only be described by the same structure whose activity is being evaluated, the institution may lack defensible oversight evidence.

That does not mean every governance process must be adversarial. It means the structure should not depend on self-validation.

IX. Oversight Evidence: The Record of Governance

The fifth requirement is oversight evidence.

Cyber governance must leave a record. But not every record is a governance record.

An institution may have technical logs, incident tickets, project plans, meeting minutes, dashboard exports, audit reports, risk registers, vendor reports, email threads, and policy documents. These records may be useful. They may show activity. They may support reconstruction. They may help explain operational response.

But oversight evidence must do something more specific.

It must demonstrate that governance occurred.

Oversight evidence should show that decision rights were defined, escalation expectations were established, accountability was assigned, materiality was considered, executive or board awareness occurred when required, risk acceptance was authorized, independent review was used where appropriate, follow-up obligations were tracked, and

institutional memory was preserved.

This is also where board guidance and governance architecture must be distinguished. Guidance may encourage active, informed director engagement. Governance architecture determines whether that engagement leaves an institutional record capable of demonstrating oversight. A board update, cyber briefing, or committee discussion may be useful, but it becomes stronger governance evidence when it is connected to defined authority, escalation expectations, accountability assignments, documented challenge, follow-through obligations, and a record of the decision or oversight function performed.

This evidence should exist before the institution is asked to defend its decisions.

After a cyber event, enforcement inquiry, insurer dispute, audit review, customer challenge, litigation process, or board question, the institution may need to demonstrate not only what happened, but how the relevant decisions were governed.

If the governance record is constructed only after the event, the institution is not demonstrating oversight. It is reconstructing it.

Defensible oversight begins before pressure arrives.

X. Cybersecurity Maturity Is Not Governance Maturity

Many organizations measure cyber maturity through frameworks, control coverage, assessments, tooling, training, incident response capability, and remediation progress. These measures have value. They are necessary to understanding operational capability.

But cybersecurity maturity is not the same as governance maturity.

Cybersecurity maturity asks whether the program is capable. Governance maturity asks whether the institution can demonstrate how material cyber risk is governed.

The difference is substantial.

A mature security program may still lack formal decision-rights architecture, board-level escalation thresholds, clear accountability for risk acceptance, independent validation of governance claims, evidence of oversight before consequential events, or stable language connecting cyber risk to enterprise governance.

This is why cyber governance cannot be reduced to security maturity reporting. A board should not be satisfied only with better metrics. It should ask whether those metrics are tied to authority, escalation, accountability, and evidence.

A mature cyber program may answer the question: “Are we doing the work?”

A mature governance architecture answers the question: “Can we demonstrate how the institution governed the decisions that mattered?”

Both questions matter.

They are not the same question.

XI. The CRGA™ Governance Architecture Requirement

CRGA™ Governance Architecture defines how boards and executives govern material technology-enabled enterprise risk through decision rights, escalation discipline, accountability architecture, structural independence, stable governance language, and defensible oversight evidence.

In the cyber context, this architecture reframes the enterprise question.

The question is not only whether the organization has a cybersecurity program. It is whether the institution can demonstrate that cyber risk is governed at the level of authority, escalation, accountability, and oversight evidence.

That requires the institution to define which cyber decisions are governance decisions, who has authority to make or escalate them, which conditions require executive or board attention, who is accountable for outcomes and decisions, what evidence demonstrates oversight, and how the institution maintains independence between execution and validation.

This architecture does not replace operational cybersecurity. It governs the institutional conditions under which operational cybersecurity becomes accountable.

The distinction is important. Praesidium does not argue that governance architecture substitutes for technical competence, operational execution, or security program maturity. It argues that those capabilities operate inside an institutional structure that must define authority, escalation, accountability, and evidence.

Without that structure, operational security may remain disconnected from fiduciary oversight.

With that structure, cyber risk can be governed as enterprise risk.

XII. Board-Level Application

Boards and executives can begin reframing cyber risk governance by asking a different set of questions.

The board should not only ask whether the organization is secure. It should ask how cyber risk is governed. It should not only ask what the dashboard shows. It should ask what decision the information triggers. It should not only ask what controls are in place. It should ask who has authority to accept, defer, escalate, or challenge the risk. It should not only ask whether management reported the issue. It should ask whether escalation was required under defined conditions. It should not only ask who was involved. It should ask who was accountable. It should not only ask what documentation exists. It should ask what evidence demonstrates that oversight occurred.

These questions do not require directors to operate cybersecurity. They require the institution to demonstrate that cyber risk decisions are governed.

That is the board-level shift.

The board's role is not to become the cybersecurity function. The board's role is to ensure that the institution has an architecture capable of converting cyber risk information into governed decisions, assigned accountability, timely escalation, and defensible oversight evidence.

When that architecture exists, boards are better positioned to oversee cyber risk without overstepping into management. When it does not exist, boards may receive more information without gaining meaningful governance clarity.

That is why the transition from operational security to fiduciary oversight matters.

XIII. Implications for Institutions

The movement from operational security to fiduciary oversight has practical implications for how institutions design, document, and review cyber risk governance.

First, institutions should distinguish cyber program maturity from cyber governance maturity. A capable program is necessary, but it does not answer every oversight question. The institution should evaluate whether its cyber program is connected to decision rights, escalation thresholds, accountability assignments, independent validation, and oversight evidence.

Second, institutions should define governance materiality before events occur. If materiality is interpreted only after an incident, the organization may be reconstructing its governance position under pressure. Materiality should not live only inside technical severity ratings, legal analysis, or tool settings. It should be reflected in the governance architecture.

Third, institutions should ensure that board reporting is tied to governance action. A dashboard should not merely inform the board. It should operate within a structure that defines what the information means, who must act on it, when escalation is required, and how the response will be evidenced.

Fourth, institutions should preserve independence between execution and validation. The same structure should not be expected to define the standard, perform the work, report the result, and validate its own adequacy without appropriate governance checks.

Finally, institutions should design oversight evidence before pressure arrives. Evidence should not be treated as a post-event documentation exercise. It should be a deliberate feature of governance architecture.

These implications are not administrative preferences. They are the conditions that allow cyber risk to become governable at the enterprise level.

CONCLUSION

Cyber risk is no longer adequately governed through operational security alone.

The institution still needs strong controls, skilled teams, effective tools, mature processes, credible vendors, and disciplined incident response. Those capabilities remain essential. But they are not substitutes for governance architecture.

The enterprise question has changed.

Institutions are increasingly not judged solely by whether cyber incidents occur. They are judged by whether they can demonstrate that cyber risk was governed.

That demonstration requires more than visibility, activity, maturity scores, frameworks, or reports. It requires a governance architecture capable of defining who had authority, when escalation was mandatory, how accountability was assigned, whether validation was independent, and what evidence demonstrates oversight.

The shift from operational security to fiduciary oversight is the shift from asking whether the organization acted to asking whether the institution governed.

That is the architecture Praesidium defines through CRGA™.

EXTERNAL REFERENCE

National Association of Corporate Directors and Internet Security Alliance, *Director's Handbook on Cyber-Risk Oversight*, Fifth Edition, 2026.
Praesidium references the NACD/ISA handbook as external board-governance guidance reflecting the continued maturation of cyber-risk oversight expectations. Praesidium does not reproduce, modify, adopt, or incorporate NACD/ISA principles, tools, frameworks, or visual materials. The reference is used solely to support the broader market observation that cyber risk has become a board-level governance issue. Praesidium Governance, Inc. is not affiliated with, endorsed by, sponsored by, certified by, or otherwise approved by NACD or ISA.