American Journal of Advanced Multidisciplinary Innovation and Research (AJAMIR)

E-ISSN: XXXX-XXXX ● Website: www.ajamir.com ● Email: editor@ajamir.com

Cyber-Risk Communication and Executive Decision Quality

Dr. Lukas M. Schneider

Professor, Technical University of Munich, Germany

Abstract

Cybersecurity risk is increasingly an enterprise governance issue rather than an isolated technical concern. Senior executives and boards must make decisions about security investment, incident escalation, business interruption, risk acceptance, cyber insurance, third-party exposure, regulatory disclosure, and recovery priorities, yet the information supporting those decisions is frequently communicated through vulnerability counts, technical severity ratings, control deficiencies, and threat terminology that may not directly express consequences for enterprise objectives. Current NIST guidance explicitly connects cybersecurity risk management with enterprise risk management and emphasizes the need for directors and senior leaders to understand cybersecurity risk posture in relation to mission and business objectives. The December 2025 revision of NIST IR 8286 further strengthens the connection among cybersecurity risk registers, enterprise risk processes, governance, and executive decision-making.

This study investigates how the format of cyber-risk communication may influence executive decision quality. Four hypothetical communication conditions were modeled: technical metrics only, traffic-light risk summaries, business-impact narratives, and integrated executive decision briefs combining threat scenarios, business consequences, uncertainty, risk appetite, residual risk, response alternatives, and explicit decision requirements. A synthetic experiment representing 480 executive decision episodes was constructed, with 120 episodes allocated to each communication format. Decision quality was assessed through risk comprehension, prioritization accuracy, decision confidence, timeliness, uncertainty calibration, and overall decision-support effectiveness. The integrated decision brief achieved the highest simulated composite score of 88.8, compared with 55.6 for technical metrics, 66.6 for traffic-light reporting, and 78.8 for business-impact narratives. The strongest condition also generated the lowest modeled misprioritization rate and the highest alignment between executive decisions and predefined organizational risk tolerance.

The study does not argue that executives should receive less technical information. Instead, it proposes a layered communication architecture in which technical evidence remains auditable while the executive layer translates that evidence into scenarios, mission consequences, financial and operational exposure, uncertainty ranges, response options, residual risk, and a clearly defined decision. This approach is consistent with NIST's enterprise-risk guidance and with research showing that scenario-based engagement can reveal executive cyber-risk perceptions and preparedness more effectively than abstract technical discussion alone. The paper concludes that high-quality cyber-risk communication is

American Journal of Advanced Multidisciplinary Innovation and Research (AJAMIR)

E-ISSN: XXXX-XXXX ● Website: www.ajamir.com ● Email: editor@ajamir.com

not merely a reporting activity; it is a decision architecture that can materially shape how leaders allocate resources and respond to uncertainty.

Keywords: cyber-risk communication, executive decision-making, cybersecurity governance, enterprise risk management, board oversight, risk communication, cyber resilience, cybersecurity strategy, business impact, executive cyber literacy

1. Introduction

Cybersecurity has moved from a predominantly operational information-technology concern into the domain of enterprise governance. Digital dependence means that cyber incidents can affect revenue, operational continuity, regulatory exposure, intellectual property, customer trust, supply chains, strategic projects, and organizational reputation. Contemporary governance frameworks consequently expect senior leaders to understand and oversee cybersecurity as part of broader enterprise risk management. NIST's revised IR 8286 series states that directors and senior leaders need a clear understanding of cybersecurity risk posture and that cybersecurity risks should be assessed in the context of broader mission and business objectives. For U.S. public companies, SEC cybersecurity disclosure rules similarly require disclosure regarding processes for assessing and managing material cybersecurity risk, management's role in that process, and the board's oversight of cybersecurity risk.

The governance challenge is not simply that cyber risks are difficult to detect. It is that cyber specialists and executives often operate with different decision vocabularies. Security teams may discuss vulnerabilities, attack paths, control maturity, exploitability, threat actors, authentication failures, patching exposure, and detection coverage. Executives typically need to determine whether a risk threatens a strategic objective, whether additional investment is justified, which business process is exposed, how much disruption is tolerable, whether risk can be accepted or transferred, and what action should occur now. NIST's business-impact guidance specifically links mission-essential functions, risk appetite, impact analysis, prioritization, response, and communication, illustrating why cybersecurity information must eventually be translated into the terms through which enterprise decisions are made.

The difficulty is intensified by uncertainty. Cybersecurity decisions frequently occur without reliable probabilities, complete loss estimates, or full knowledge of attacker intent. Brantly argues that risk and uncertainty need to be distinguished analytically in cyberspace because decision-makers often operate in environments where uncertainty cannot be reduced to conventional probabilistic risk. Cyber-loss research likewise shows that cybersecurity losses can be heavy-tailed, meaning that relatively infrequent incidents may generate disproportionately severe outcomes. Consequently, an executive briefing that presents a single precise risk score may create an impression of certainty that the underlying evidence does not support.

Communication quality also affects the relationship between cyber specialists and organizational leadership. Parkin, Kuhn, and Shaikh's scenario-driven study with executive decision-makers showed that cyber-risk perception and preparedness can be explored through realistic incident scenarios rather than relying only on abstract risk statements. Harel's 2025 strategic cybersecurity oversight framework similarly emphasizes board-level sensemaking and structured oversight of cybersecurity threats. These

studies suggest that executive communication should support interpretation and choice rather than merely transfer information from specialists to leaders.

The present study therefore examines Cyber-Risk Communication and Executive Decision Quality through a simulation-based comparative framework. Its central proposition is that cyber-risk reporting should be evaluated according to whether it enables a senior decision-maker to understand the scenario, compare the risk with organizational priorities and tolerance, interpret uncertainty, evaluate response alternatives, and make a timely decision. Four communication formats are compared to determine how progressively stronger translation from technical cybersecurity evidence to enterprise decision information could influence executive decision quality.

2. Objectives of the Study

2.1 To Examine the Relationship Between Cyber-Risk Communication Format and Executive Understanding

The first objective is to compare technical, summarized, business-oriented, and integrated communication approaches according to their ability to support executive comprehension of cyber-risk scenarios, consequences, uncertainty, and organizational relevance.

2.2 To Evaluate Communication Effects on Prioritization and Decision Quality

The second objective is to examine how different cyber-risk communication structures influence prioritization accuracy, decision confidence, response timeliness, uncertainty calibration, and alignment with predefined organizational risk tolerance.

2.3 To Develop an Executive Cyber-Risk Decision Briefing Framework

The third objective is to construct a practical communication architecture connecting technical cybersecurity evidence with business impact, strategic objectives, residual risk, uncertainty, response alternatives, decision ownership, and governance follow-up.

3. Review of Literature

3.1 Cybersecurity Risk Communication and Enterprise Risk Management

Cybersecurity risk communication becomes strategically meaningful when technical risks are integrated into enterprise risk management rather than managed as an isolated technology portfolio. NIST IR 8286 Rev. 1, finalized in December 2025, explicitly frames cybersecurity risk management as an input to broader enterprise-risk processes and highlights cybersecurity risk registers as mechanisms for organizing and aggregating information relevant to enterprise objectives. NIST IR 8286C Rev. 1 further addresses the staging and aggregation of cybersecurity risks for enterprise risk management and governance oversight.

This integration is important because organizational leaders allocate limited resources across different risk categories. Cybersecurity therefore competes and interacts with operational, financial, legal, supply-chain, strategic, and reputational risks. A technical vulnerability may be strategically minor if it affects a low-value isolated system, whereas a moderate technical weakness may be critical if it compromises a mission-essential business service. NIST's updated business-impact guidance supports

this reasoning by connecting mission-essential functions with impact analysis, risk appetite, prioritization, response, and communication.

Enterprise communication consequently requires an appropriate level of aggregation. Executives generally should not need to interpret every vulnerability record, yet excessive aggregation can erase important uncertainty or dependency information. NIST's revised risk-management series addresses this problem through cybersecurity risk registers and enterprise risk profiles that allow operational evidence to be rolled upward without removing the connection to underlying risk detail.

The executive communication problem is therefore not solved by either technical detail or simplification alone. A useful briefing needs selective detail: enough evidence to justify the assessment, enough enterprise context to establish importance, and enough uncertainty information to prevent oversimplified conclusions.

3.2 Executive Risk Perception, Scenario Framing, and Decision-Making

Risk perception influences how leaders interpret cybersecurity information. Individuals do not necessarily respond to identical risk information in identical ways because prior experience, organizational role, perceived controllability, strategic pressure, and consequence framing affect judgment. Cybersecurity adds technical complexity and adversarial uncertainty to these established decision challenges.

Parkin, Kuhn, and Shaikh used scenario-based workshops with organizational executives to examine cyber-risk perceptions relating to incident preparation and response. Their methodology demonstrates the value of concrete scenarios in revealing leadership assumptions and decision capacities. A scenario provides more decision-relevant structure than a standalone statement such as “ransomware risk is high” because it can explain which operations are threatened, how long disruption could continue, what recovery resources are available, and what decisions are required.

Harel's strategic cybersecurity oversight framework extends this concern to boards, proposing a structured sensemaking approach for cybersecurity oversight. Sensemaking is particularly relevant when cybersecurity evidence is incomplete because leaders need to form a coherent interpretation of the situation before deciding whether to accept, mitigate, avoid, or transfer the risk.

Current risk conditions reinforce the need for high-quality executive communication. The World Economic Forum's 2026 cybersecurity outlook reports that AI-related vulnerabilities were identified by 87% of respondents as the fastest-growing cyber risk during 2025. The Forum's 2025 work likewise emphasized increasing complexity created by geopolitical conditions, supply-chain interdependence, emerging technologies, and increasingly sophisticated cybercrime. Such conditions make static annual cybersecurity presentations less useful than communication processes capable of updating executive understanding as the threat and business environment changes.

3.3 Materiality, Uncertainty, and Executive Action

Cyber-risk communication has consequences beyond internal investment. Leaders may need to determine whether an incident is financially material, whether operations should be suspended, whether external parties should be notified, whether a ransom or recovery strategy should be considered, and whether risk should be escalated to the board.

The SEC's cybersecurity disclosure framework provides a concrete example of how cyber-risk communication interacts with executive judgment. Public companies subject to the rules must disclose specified material cybersecurity incidents and describe cybersecurity risk-management and governance processes. The incident disclosure requirement is generally triggered within four business days after the registrant determines that an incident is material, rather than four days after the technical event itself. Accurate and rapid translation from incident evidence to enterprise consequence therefore becomes important for governance and disclosure decisions.

Uncertainty complicates materiality and prioritization because many impacts remain unknown during early incident stages. Cyber-loss evidence suggests that incident severity distributions can include extreme outcomes, reducing the usefulness of simple average-loss expectations. Executives may therefore need ranges, scenarios, confidence levels, and explicit assumptions rather than one deterministic expected-loss number.

The literature consequently supports decision-oriented communication containing at least five layers: the cyber scenario, the affected business objective, the potential consequence, the uncertainty associated with the estimate, and the available response. The present study operationalizes these layers within its integrated executive decision brief.

4. Research Methodology

4.1 Research Design and Synthetic Executive Decision Sample

The study adopts a simulation-based comparative research design. A total of 480 synthetic executive decision episodes were created, representing hypothetical decisions involving ransomware, cloud-service compromise, third-party supply-chain intrusion, privileged-account takeover, sensitive-data exposure, and major business-service disruption.

The scenarios were designed to require executive choices rather than purely technical remediation. Decisions included accepting residual risk, approving security investment, temporarily suspending an operational service, escalating an incident to the board, activating a crisis-management structure, or funding an accelerated resilience measure.

The 480 decision episodes were divided equally among four communication conditions, giving 120 simulated executive decisions per format.

Table 1: Experimental Cyber-Risk Communication Conditions

Communication Condition	Information Presented	Main Communication Characteristic	Expected Decision Limitation
Technical metrics only	Vulnerability severity, attack indicators, control failures, affected systems, technical likelihood	High technical detail	Weak translation to enterprise consequence
Traffic-light	Red/amber/green risk status, short	Rapid	Potential loss of

Communication Condition	Information Presented	Main Communication Characteristic	Expected Decision Limitation
summary	ranking, selected key risk indicators	simplification	uncertainty and causal detail
Business-impact narrative	Cyber scenario linked to operational, financial, regulatory, and reputational consequences	Enterprise-oriented interpretation	Response options may remain insufficiently structured
Integrated executive decision brief	Scenario, business objective, impact range, uncertainty, risk appetite/tolerance, residual risk, response alternatives, decision deadline, recommendation	Decision-centered communication	Higher preparation and governance discipline required

Source: Author's simulation framework informed by NIST enterprise-risk guidance, scenario-based executive cybersecurity research, and contemporary governance literature.

4.2 Executive Decision Quality Measures

Six outcome measures were defined.

- Risk comprehension represented whether the executive correctly identified the relevant cyber scenario, affected business objective, and principal consequence.
- Prioritization accuracy measured whether the risk was ranked consistently with the simulated organization's predefined business-criticality and risk-tolerance structure.
- Decision confidence represented the decision-maker's ability to select and justify a response without requiring unnecessary additional clarification.
- Decision timeliness measured the extent to which the decision occurred within the time required by the simulated incident or risk-management process.
- Uncertainty calibration represented whether the decision reflected the actual level of uncertainty built into the scenario rather than treating low-confidence estimates as precise facts.
- Decision-support effectiveness was calculated from the preceding measures and the proportion of decisions aligned with the simulated risk appetite.

All outcome scores were standardized to a 0–100 scale for methodological comparability.

4.3 Simulation Procedure and Analytical Boundaries

Each risk scenario was first represented as a common technical evidence package. The content was then transformed into the four communication formats without changing the underlying risk condition.

For example, a technical report might state that a critical identity-management system contained an exploitable vulnerability with privileged-access implications. The traffic-light format would classify

American Journal of Advanced Multidisciplinary Innovation and Research (AJAMIR)

E-ISSN: XXXX-XXXX ● Website: www.ajamir.com ● Email: editor@ajamir.com

the issue as red. The business-impact narrative would explain that compromise could interrupt customer onboarding and expose regulated personal information. The integrated decision brief would additionally state the plausible impact range, confidence in the estimate, current controls, residual risk, relevant risk tolerance, alternative responses, cost implications, decision owner, and required decision time.

Synthetic decision responses were generated under controlled distributions reflecting the information content of each condition. No claim is made that real executives would produce the exact same differences.

No inferential p-values are reported because the observations were deliberately simulated. A real empirical study should recruit executives or senior managers, randomize communication formats, use equivalent risk scenarios, preregister decision-quality criteria, and separately measure cybersecurity experience, financial expertise, and risk preferences.

5. Analysis

5.1 Comparative Executive Decision Quality

Technical metrics alone produced the weakest overall simulated performance. Risk comprehension reached 58, prioritization accuracy 54, decision confidence 56, timeliness 61, and uncertainty calibration

The traffic-light format improved rapid recognition of urgent risks and increased decision timeliness to 75. However, uncertainty calibration remained comparatively weak at 55, illustrating a potential limitation of compressed red-amber-green reporting. A red rating can communicate urgency efficiently while obscuring whether underlying estimates are robust or highly uncertain.

Business-impact narratives generated a substantial improvement. Risk comprehension increased to 82, prioritization accuracy to 80, and uncertainty calibration to 72.

Table 2: Simulated Executive Decision Outcomes by Cyber-Risk Communication Format

Communication Format	Risk Comprehension	Prioritization Accuracy	Decision Confidence	Decision Timeliness	Uncertainty Calibration	Composite Decision Quality
Technical metrics only	58	54	56	61	49	55.6
Traffic-light summary	69	66	68	75	55	66.6
Business-impact narrative	82	80	79	81	72	78.8
Integrated executive decision brief	91	89	88	90	86	88.8

American Journal of Advanced Multidisciplinary Innovation and Research (AJAMIR)

E-ISSN: XXXX-XXXX ● Website: www.ajamir.com ● Email: editor@ajamir.com

5.2 Why Business Translation Improves Prioritization

The increase from 55.6 under technical reporting to 78.8 under business-impact communication is driven primarily by improved risk comprehension and prioritization.

A technical severity score answers a cybersecurity question: how serious is a vulnerability or threat from a technical perspective? It does not necessarily answer the enterprise question: how much does the associated scenario matter to the organization's objectives?

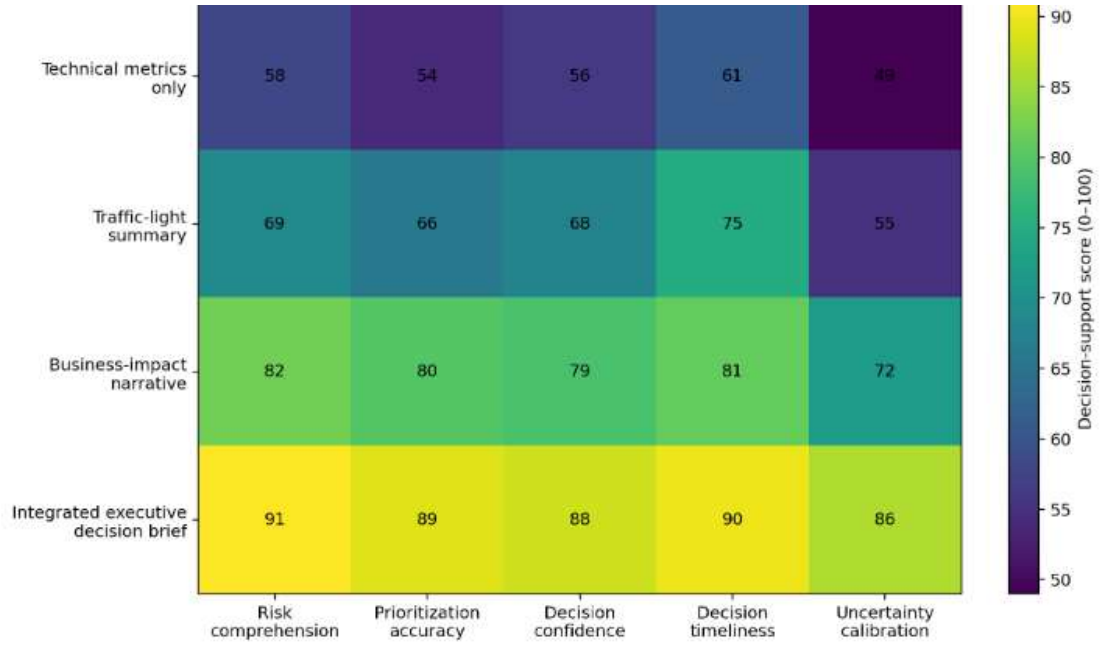
NIST's current enterprise-risk guidance supports precisely this transition. The IR 8286 series connects system-level cybersecurity risk information with broader enterprise-risk registers and profiles, while NIST IR 8286D uses business impact analysis to establish how critical assets and risk scenarios affect mission objectives.

The integrated briefing condition further improves decision quality by including response alternatives. Executives are not merely informed that a risk is significant; they are asked to select among explicit actions such as mitigate immediately, accept temporarily, transfer part of the risk, postpone an initiative, or authorize additional resilience investment.

This shifts communication from risk presentation to decision support.

5.3 Executive Decision-Support Heatmap

Graph 1: Simulated Executive Decision Quality Across Cyber-Risk Communication Formats



The heatmap demonstrates the multidimensional character of communication quality. Technical reporting performs comparatively weakly across all five decision-support variables despite containing detailed cybersecurity information.

Traffic-light reporting improves timeliness but produces only limited improvement in uncertainty calibration. This pattern illustrates why status dashboards can be valuable as attention-directing devices

Business-impact narratives perform substantially better because they express cyber risks through organizational consequences.

The integrated executive decision brief produces the strongest and most balanced profile because it combines enterprise translation with decision structure and uncertainty.

The key analytical finding is therefore that executive decision quality appears strongest when cyber-risk communication tells leaders not only what the technical problem is, but why it matters, how certain the assessment is, how the risk compares with organizational tolerance, and what decision is required.

6. Discussion

6.1 Cyber-Risk Communication Should Be Designed Around Decisions Rather Than Reports

The simulated findings indicate that executive cyber-risk communication becomes more useful when the communication process begins with the decision that leadership must make rather than with the cybersecurity information that specialists wish to report. This distinction changes the architecture of an executive briefing. A conventional technical presentation may begin with vulnerabilities, incidents, threat actors, patching levels, and security controls and expect executives to derive the business implications. A decision-oriented briefing works in the opposite direction: it begins by identifying the organizational objective potentially affected, defines the cyber scenario that threatens that objective, and then provides the technical evidence required to justify the risk assessment. This direction is consistent with NIST IR 8286 Rev. 1, which integrates cybersecurity risk information into the broader enterprise-risk context rather than treating cyber risk as an independent reporting domain.

Decision-oriented communication also clarifies the difference between information completeness and information usefulness. Senior leaders should have access to sufficient technical evidence, but an executive briefing does not need to reproduce the entire cybersecurity risk register. NIST IR 8286C Rev. 1 specifically addresses the aggregation and staging of cybersecurity risk information for enterprise and governance oversight. A layered model is therefore appropriate. Technical teams maintain detailed evidence and risk records; managers aggregate related scenarios; and executives receive an enterprise-level view with the ability to drill down when necessary. Such a system preserves traceability without requiring leaders to interpret operational telemetry directly.

Scenario framing is particularly useful because it links abstract cyber threats to recognizable business conditions. Parkin and colleagues' executive workshop research demonstrates the practical value of scenario-based approaches for assessing cyber-risk perception and organizational preparedness. An executive is likely to reason more effectively about “loss of the customer identity platform for forty-eight hours during peak enrollment” than about “critical identity infrastructure risk” alone because the scenario establishes the asset, consequence, timeframe, and organizational dependency through which the decision becomes concrete.

6.2 Simplification Must Not Remove Uncertainty or Residual Risk

The traffic-light condition in the simulation illustrates an important communication hazard. Red, amber, and green classifications are attractive because they allow executives to identify areas requiring attention quickly. Their weakness arises when categorical status replaces the information needed to interpret uncertainty. Two cyber risks may both be labeled red even though one is supported by strong incident evidence and the other is based on an emerging but highly uncertain threat scenario. Treating those conditions as equivalent can lead to misallocation of resources.

Cybersecurity uncertainty should therefore be communicated explicitly. This does not require presenting executives with complex probability theory. Useful approaches include ranges, confidence labels, scenario bands, clearly identified assumptions, and distinctions between known facts and analyst judgments. Brantly's analysis of risk and uncertainty in cyberspace supports the conceptual importance of distinguishing uncertain conditions from conventionally quantified risk. The heavy-tailed nature observed in cyber-loss research provides a second reason to avoid overreliance on single expected-loss figures because severe cyber outcomes may remain important even when estimated event frequency is low.

Residual risk should be communicated with equal care. Executives do not primarily decide whether a security control is technically effective; they decide whether the remaining risk after controls is acceptable relative to enterprise objectives and risk appetite. NIST's business-impact approach connects enterprise risk directives, including risk appetite and tolerance, with asset criticality and risk response. An executive briefing should therefore state the risk before treatment, the control or investment being proposed, the expected residual risk, and the uncertainty around that expectation. Without residual-risk communication, cyber investment decisions may become falsely binary, implying that a proposed control either solves the problem or provides no value.

6.3 Executive Cyber Communication Should Function as a Governance Loop

The strongest communication model should not terminate once an executive approves or rejects a recommendation. A mature process records the decision, assumptions, risk acceptance conditions, responsible owner, expected control effect, performance indicator, and date for reconsideration. Cyber-risk communication then becomes a governance loop in which technical teams report changing conditions, management reassesses residual risk, and executives adjust strategic direction when risk moves outside agreed tolerance.

This cyclical model aligns with contemporary cybersecurity governance. The SEC's cybersecurity rules require disclosure concerning management's role in assessing and managing material cybersecurity risks and the board's oversight of those risks, illustrating the institutional importance of established reporting and oversight channels. NIST's revised IR 8286 framework likewise emphasizes enterprise-level risk information and governance oversight rather than isolated technical reporting.

Current threat complexity strengthens the case for this continuous governance model. The World Economic Forum's 2025 and 2026 cybersecurity outlooks emphasize changing risks associated with AI, supply-chain interdependence, geopolitical conditions, cybercrime, and digital fraud. An annual board presentation cannot adequately represent a risk environment that changes continuously. Executive

communication should therefore combine scheduled strategic reporting with predefined escalation thresholds for material changes in exposure.

The present study remains simulation-based, and its numerical differences should not be interpreted as causal evidence from real boards. Future research should conduct controlled experiments with executives and board members, compare numerical and narrative risk formats, test the influence of financial ranges and uncertainty labels, measure decision latency during simulated incidents, and examine whether communication formats produce different effects among executives with different cybersecurity expertise. Such research would provide stronger evidence regarding which briefing structures actually improve governance outcomes.

7. Conclusion

Cybersecurity governance depends not only on the quality of technical security controls but also on the quality of decisions through which organizations allocate resources, accept risks, prioritize recovery, manage incidents, and establish resilience. Executives cannot make these decisions effectively when cybersecurity information remains disconnected from organizational objectives.

The simulation presented in this study demonstrates a progressive relationship between cyber-risk communication structure and modeled executive decision quality. Technical metrics produced a composite score of 55.6, traffic-light summaries 66.6, business-impact narratives 78.8, and integrated executive decision briefs 88.8. These scores are synthetic and should not be interpreted as empirical findings. Their value lies in demonstrating how executive communication can be evaluated through comprehension, prioritization, confidence, timeliness, and uncertainty calibration rather than through information volume alone.

The strongest model preserves technical evidence but translates it through a structured decision layer. An effective executive cyber-risk brief should identify the relevant business objective, describe the cyber scenario, explain operational and financial consequences, state what is known and uncertain, compare residual risk with organizational tolerance, present realistic response alternatives, identify the accountable decision-maker, and specify when the decision must occur.

This structure also prevents oversimplification. Cyber risk should not be reduced to an unexplained red status or a single dollar figure. Uncertainty, assumptions, scenario ranges, and residual exposure should remain visible enough for executives to understand what the assessment can and cannot establish.

Cyber-risk communication should additionally continue after the decision. Accepted risks require review, approved controls require performance monitoring, and executive assumptions require reconsideration as technology, threat actors, suppliers, and organizational priorities change. This transforms cyber communication from periodic presentation into an active governance process.

The principal conclusion is therefore that effective cyber-risk communication is a form of decision engineering. Its purpose is not simply to make cybersecurity easier for executives to understand. Its purpose is to organize technical evidence so that leaders can make timely, proportionate, auditable, and strategically aligned decisions under uncertainty.

References

1. Chen, J. (2020). Risk communication in cyberspace: A brief review of the information-processing and mental models approaches. *Current Opinion in Psychology, 36,* 135–140. https://doi.org/10.1016/j.copsyc.2020.06.006.
2. Zhang, X. A., & Borden, J. (2020). How to communicate cyber-risk? An examination of behavioral recommendations in cybersecurity crises. *Journal of Risk Research, 23*(10), 1336–1352. https://doi.org/10.1080/13669877.2019.1646315.
3. Daza, R., & Hargiss, K. M. (2018). Factors comprising effective risk communication, decision-making, and measurement of IT and IA risk. *International Journal of Strategic Information Technology and Applications, 9*(1), 23–40. https://doi.org/10.4018/IJSITA.2018010102.
4. Ashenden, D., & Sasse, M. A. (2013). CISOs and organizational culture: Their influence on information security management. *Proceedings of the 8th International Conference on Availability, Reliability and Security,* 40–47.
5. Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *International Conference on Cyber Security for Sustainable Society*, 1–15.
6. Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management, 51*(2), 217–224.
7. Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly, 34*(3), 549–566.
8. Johnston, A. C., & Siponen, M. (2018). Speak their language: Designing effective messages to improve employees' information security decision making. *Decision Sciences, 50*(2), 245–284. https://doi.org/10.1111/deci.12328.
9. Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523–548.
10. Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems, 18*(2), 106–125.
11. Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). A model for evaluating IT security investments. *Communications of the ACM, 47*(7), 87–92.
12. Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security, 5*(4), 438–457.
13. Anderson, R., & Moore, T. (2006). The economics of information security. *Science, 314*(5799), 610–613.
14. Shedden, P., Ruighaver, A. B., & Ahmad, A. (2011). Organizational security culture: Extending the end-user perspective. *Computers & Security, 30*(1), 35–44.
15. Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly, 34*(3), 487–502.
16. Straub, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research, 1*(3), 255–276.

17. Werlinger, R., Hawkey, K., & Beznosov, K. (2009). An integrated view of human, organizational, and technological challenges of IT security management. *Information Management & Computer Security, 17*(1), 4–20.
18. Couce-Vieira, A., Ríos Insua, D., & Kosgodagan, A. (2020). Assessing and forecasting cybersecurity impacts. *Decision Analysis, 17*(4), 356–374. https://doi.org/10.1287/deca.2020.0418.
19. Ahmad, A., Maynard, S. B., & Park, S. (2014). Information security strategies: Towards an organizational multi-strategy perspective. *Journal of Intelligent Manufacturing, 25*, 357–370.
20. AlHogail, A. (2015). Design and validation of information security culture framework. *Computers in Human Behavior, 49*, 567–575.