iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
https://ijetrm.com/

THE CYBERSECURITY DESIGN GAP: EXAMINING WHY ORGANIZATIONS FAIL TO ACT ON IDENTIFIED CYBER RISKS

Mojisola Ologe
Coauthor: Aisha Abdullahi

ABSTRACT
Organizations increasingly rely on cybersecurity assessments, vulnerability scanners, penetration tests, compliance audits, and threat intelligence to identify weaknesses in their digital environments. Yet identifying a risk does not guarantee that the organization will address it. Significant vulnerabilities may remain unresolved because responsibility is unclear, remediation competes with operational priorities, budgets are constrained, technical teams lack authority, or managers underestimate uncertain future losses. This paper examines the organizational, managerial, economic, behavioural, and technical factors that contribute to the gap between identifying cybersecurity risks and implementing effective responses. It conceptualizes the cybersecurity design gap as a failure in the organizational arrangements through which identified risks are evaluated, assigned, prioritized, authorized, treated, and verified. Drawing on cybersecurity risk management standards and literature on security economics, organizational governance, decision-making, and resource capabilities, the paper develops an integrated conceptual framework for explaining why risks remain unresolved. The framework distinguishes justified risk treatment decisions from unauthorized acceptance, avoidable delay, and implementation failure. It proposes a stage-based response process, clarifies decision-making responsibilities, and recommends measures that assess remediation quality rather than merely counting closed security tickets. The paper contributes a structured basis for improving cybersecurity risk-response decisions and proposes empirical approaches for future validation. As a conceptual literature-based study, its framework is intended for subsequent testing rather than presented as an empirically validated model.

Keywords:
cybersecurity risk management, vulnerability remediation, risk-response decisions, organizational governance, cybersecurity investment, risk acceptance, security economics

I. INTRODUCTION

1.1 Background to the Study
Cybersecurity risk management is not simply a technical exercise in identifying software vulnerabilities or detecting suspicious activity. It also involves organizational decisions about which risks require immediate attention, who has the authority to act, what resources should be committed, and which residual risks may reasonably be accepted. These decisions connect technical security assessments to business continuity, financial performance, regulatory obligations, and organizational reputation. Established frameworks recognize this connection. The National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0 places governance alongside the identification, protection, detection, response, and recovery functions, emphasizing that cybersecurity decisions should reflect organizational objectives and risk priorities (Pascoe et al., 2024). Similarly, NIST's Risk Management Framework links system-level security activities with organizational decision-making and accountability (Joint Task Force, 2018).

Nevertheless, the availability of risk information does not ensure effective action. An organization may know that a publicly accessible server contains a serious vulnerability, for example, but postpone remediation because the server supports a critical business application that cannot easily be taken offline. In another organization, a risk assessment may be completed and a treatment plan approved, yet the required funds or technical personnel may never be assigned. In both cases, the risk is known, but the organizational process has not translated that knowledge into a verified reduction in exposure. The distinction matters because cybersecurity tools primarily reveal or help assess weaknesses; they cannot independently resolve competing departmental interests, authorize expenditure, establish accountability, or determine acceptable business disruption. These are organizational and managerial responsibilities, even when the underlying risk is technical.

 © Author(s) | CC BY 4.0 International License.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
https://ijetrm.com/

1.2 Statement of the Problem

A persistent challenge in cybersecurity governance is the gap between the identification of risks and the implementation of appropriate responses. Existing guidance describes risk assessment, control selection, authorization, monitoring, and continuous improvement, while research on cybersecurity investment demonstrates that economic incentives and interdependence can influence organizational security decisions (Anderson & Moore, 2006; Fedele & Roner, 2022). Research on cybersecurity investment incentives also identifies economic, normative, historical, and feasibility-related influences on the adoption of security measures (Niesten et al., 2021).

However, these perspectives do not automatically provide a unified explanation of how organizational barriers interact across the full risk-response process. A lack of resources may prevent implementation, but unclear accountability may prevent the organization from securing those resources in the first place. Similarly, managers may approve a treatment plan without understanding its operational implications, while technical teams may complete a task without verifying whether the original risk has materially declined. The central problem, therefore, is not simply that organizations possess vulnerabilities. It is that their decision-making and implementation arrangements may fail to convert credible risk information into timely, proportionate, accountable, and verified action.

1.3 Aim and Objectives

The aim of this paper is to examine why organizations fail to act effectively on identified cybersecurity risks and to develop an integrated framework for improving risk-response decisions.

The specific objectives are to:

1) Conceptualize the cybersecurity design gap and distinguish unjustified inaction from legitimate risk treatment decisions.
2) Examine the organizational, managerial, economic, behavioural, and technical factors that contribute to unresolved risks.
3) Analyze how accountability, incentives, communication, and decision-making authority influence risk treatment.
4) Explain how remediation costs, operational disruption, uncertainty, and competing priorities shape investment decisions.
5) Evaluate the contributions and limitations of established cybersecurity risk management frameworks in addressing the gap.
6) Develop a stage-based conceptual framework connecting barriers to practical interventions and measurable outcomes.
7) Propose indicators and empirical approaches for assessing the effectiveness of organizational risk responses.

1.4 Research Questions

The paper addresses seven questions:

1) What constitutes the cybersecurity design gap, and how does it differ from justified risk deferral or formal risk acceptance?
2) Which organizational, managerial, economic, behavioural, and technical factors contribute to unresolved cybersecurity risks?
3) At what stages of the risk-response process are failures most likely to arise?
4) How do accountability arrangements, managerial incentives, and resource-allocation decisions affect remediation?
5) To what extent do established cybersecurity frameworks address the organizational mechanisms that prevent action?
6) What governance and decision-support mechanisms could improve risk-response effectiveness?
7) How should organizations measure the timeliness, quality, and effectiveness of risk treatment?

1.5 Significance and Scope

The paper contributes to cybersecurity research by connecting security economics, organizational governance, and risk-management processes within a single explanatory model. For practitioners, it offers a basis for identifying why known risks remain unresolved and for assigning corrective interventions to the appropriate decision-makers.

The scope covers organizational cybersecurity risks identified through vulnerability assessments, audits, penetration testing, threat intelligence, configuration reviews, and related assurance activities. It considers risks affecting internal systems and external dependencies, including third-party services and software components. The paper does not

 © Author(s) | CC BY 4.0 International License.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
https://ijetrm.com/

assume that every finding must be remediated immediately. Instead, it examines whether the selected response is justified, authorized, adequately resourced, implemented, and verified.

II. CONCEPTUAL FOUNDATIONS

2.1 Cybersecurity Risk and Risk Treatment

Cybersecurity risk can be understood as the potential for adverse consequences arising from threats exploiting vulnerabilities in information systems, assets, processes, or dependencies. Its assessment requires consideration of the likelihood of an adverse event, its potential consequences, the effectiveness of existing controls, and the uncertainty surrounding available evidence. NIST SP 800-30 emphasizes that risk assessment should support decisions about appropriate courses of action rather than operate as an isolated technical exercise (Joint Task Force Transformation Initiative, 2012).

Identified risks can be addressed through several broad responses: mitigation, avoidance, transfer or sharing, and acceptance. Mitigation reduces the likelihood or impact of an adverse event; avoidance removes the activity or exposure that creates the risk; transfer or sharing reallocates some financial or contractual consequences; and acceptance retains the residual risk under an authorized decision. These responses are not interchangeable. Insurance, for example, may transfer certain financial losses without removing the vulnerability that permits an attack. An effective risk-response process therefore requires more than a recommendation to fix a vulnerability. It requires a reasoned decision about the available options and evidence that the chosen response achieves an acceptable outcome.

2.2 Defining the Cybersecurity Design Gap

In this paper, the cybersecurity design gap refers to a weakness in the organizational design of cybersecurity risk response: the structures, responsibilities, incentives, resources, and decision processes through which identified risks are converted into effective treatment. This definition distinguishes the concept from two related problems. A technical security design flaw concerns weaknesses in the architecture or implementation of a system. An organizational risk-response gap concerns the failure to make or execute an appropriate decision about a known risk. The two may interact, but they are not identical. A technically sound recommendation can remain unimplemented because no business owner accepts responsibility, while an organization with mature governance may still inherit a technically flawed product.

The gap should not be inferred merely because a risk remains open. An unresolved finding may reflect a legitimate maintenance window, an unavailable safe patch, a compensating control, or a documented decision to accept residual risk. The relevant question is whether the response is appropriate to the risk and supported by accountable decision-making.

Accordingly, six outcomes should be distinguished:

- Timely remediation: The risk is treated within an appropriate timeframe and the outcome is verified.
- Justified deferral: Treatment is delayed for a documented reason, with interim safeguards and a review date.
- Alternative mitigation: A different control reduces exposure when the preferred intervention is infeasible or unsuitable.
- Formal risk acceptance: An authorized decision-maker knowingly accepts the residual risk within established limits.
- Unjustified inaction: The risk remains unresolved without a defensible treatment decision or adequate interim protection.
- Implementation failure: A response is approved but is not implemented effectively or does not produce the intended reduction in risk.

This classification avoids treating risk registers as simple inventories of failure. It directs attention instead to the quality of the decision and the outcome.

2.3 The Risk-Response Process

The organizational process can be divided into seven connected stages:

1) Identification and validation: Confirm the finding, affected assets, exposure, and relevance.
2) Risk interpretation: Translate technical evidence into likely operational, financial, legal, and reputational consequences.
3) Ownership and prioritization: Assign accountable owners and determine urgency relative to other risks.
4) Decision and authorization: Select a treatment option and obtain the necessary approvals.
5) Resource allocation: Provide funding, personnel, maintenance windows, and operational support.

 © Author(s) | CC BY 4.0 International License.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
https://ijetrm.com/

6) Implementation: Execute the selected response, including technical changes and compensating measures.
7) Verification and reassessment: Test whether exposure has decreased, update residual-risk estimates, and revise the decision as conditions change.

Failures can occur at any stage and may compound across stages. A vulnerability may be accurately identified but poorly communicated; a manager may understand its importance but lack authority to fund remediation; or an approved fix may be deployed without confirming that the vulnerability has actually been eliminated.

III. LITERATURE REVIEW

3.1 Organizational Governance and Accountability

Cybersecurity risk management requires coordination among security professionals, information technology teams, business-unit leaders, asset owners, procurement personnel, and executives. These actors often possess different information and operate under different performance expectations. Security teams may prioritize reducing exposure, whereas business managers may be accountable for service availability, project delivery, or revenue targets. Yet the existence of a governance structure does not establish that accountability works in practice. An organization may designate a chief information security officer as responsible for cybersecurity while leaving the relevant business owner in control of the budget, application availability, and implementation schedule. Responsibility is then nominally centralized but operationally fragmented.

Principal–agent theory provides a useful explanation. When one party is responsible for achieving an outcome but another controls the resources or bears the immediate cost, incentives may diverge (Jensen & Meckling, 1976). A security manager may recommend an urgent upgrade, but the business-unit manager may delay it because downtime affects that unit's performance measures. The resulting delay is not necessarily caused by ignorance; it may emerge from the way authority and incentives are distributed. The literature therefore suggests that cybersecurity governance should be evaluated through actual decision rights, escalation pathways, and accountability for residual risk—not simply through the presence of policies or committees.

3.2 Managerial Priorities and Organizational Incentives

Security investments frequently compete with projects that have clearer and more immediate benefits. A new customer platform may produce visible revenue, while remediation often prevents a loss that may never occur. This asymmetry makes cybersecurity spending difficult to evaluate using short-term performance indicators alone. Niesten et al. (2021) identify multiple categories of incentives affecting cybersecurity investment, including economic, normative, historical, feasibility-related, and competing-priority influences. Fedele and Roner (2022) likewise demonstrate that security investment decisions are shaped by strategic incentives and interdependence among firms. These studies caution against assuming that organizations will always choose the security option with the greatest technical benefit.

Managerial attention is also limited. Senior leaders cannot examine every technical finding in detail, so they depend on summaries, escalation thresholds, and prioritization systems. If reports emphasize vulnerability counts, technical severity scores, or compliance status without communicating business consequences, decision-makers may struggle to distinguish urgent exposures from lower-impact issues.

A further problem occurs when managers reward teams for maintaining system availability or meeting project deadlines but do not assign equivalent accountability for unresolved security risks. In such circumstances, postponement can become the rational local choice even when it increases enterprise-wide exposure. The implication is that awareness campaigns alone are insufficient. Organizations must align security expectations with performance management, decision authority, and the incentives that influence everyday choices.

3.3 Economic Constraints and Security Investment

Cybersecurity treatment decisions involve trade-offs among expected loss reduction, implementation cost, operational disruption, and uncertainty. Gordon and Loeb (2002) demonstrate that the economically appropriate level of security investment does not necessarily increase in direct proportion to vulnerability; the cost and expected benefit of protection also matter. Their model supports the principle that organizations should evaluate security investments in relation to potential losses and the cost of reducing exposure.

Anderson and Moore (2006) further show that information security has distinctive economic characteristics, including incentives and externalities that can undermine individually rational decisions. Fedele and Roner (2022) extend this perspective through a review of cybersecurity investment models, including situations in which organizations depend on interconnected systems or influence one another's security outcomes. These insights help explain why known risks

 © Author(s) | CC BY 4.0 International License.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
https://ijetrm.com/

may remain unresolved. The direct cost of remediation is often immediate and visible, whereas the benefit is probabilistic. A patch may require testing, application downtime, vendor support, and staff time. The possible loss from exploitation is uncertain, and responsibility for that loss may be distributed across departments or external partners.

However, economic reasoning should not be reduced to a simple comparison between the cost of a fix and the expected monetary loss. Some risks are constrained by legal, regulatory, contractual, safety, or ethical requirements. A treatment that appears economically unattractive may still be mandatory. Furthermore, expected-loss estimates can be unreliable when attack likelihood, downstream effects, or recovery costs are poorly understood. The appropriate economic question is therefore not simply whether remediation is cheaper than an estimated incident. It is which feasible response offers an acceptable balance of risk reduction, cost, operational consequences, and mandatory obligations under uncertainty.

3.4 Behavioural Decision-Making and Risk Perception

Risk decisions are made by people operating with incomplete information, limited time, and competing demands. Prospect theory suggests that decision-makers evaluate uncertain outcomes through reference points and may respond differently to potential losses and gains (Kahneman & Tversky, 1979). Bounded rationality similarly recognizes that decision-makers often work with limited information-processing capacity rather than optimizing every choice (Simon, 1997).

In cybersecurity, these limitations can influence how managers interpret technical findings. A vulnerability that has not yet been exploited may appear less urgent than a current operational problem, even when the potential consequences are severe. Conversely, a highly publicized incident may draw attention away from less visible but more consequential risks elsewhere in the organization.

Communication quality matters. Technical descriptions such as severity scores, exploitability classifications, and control deficiencies may be meaningful to specialists but insufficient for executives who must allocate funds among competing business demands. Translating technical findings into plausible business scenarios can make risk information more decision-relevant.

Behavioural explanations should nevertheless be applied cautiously. A delayed decision is not automatically evidence of cognitive bias. It may reflect an unavailable patch, a difficult dependency, or a defensible assessment that immediate remediation would create greater operational risk. A robust analysis must examine the evidence, constraints, and decision record before attributing inaction to managerial psychology.

3.5 Technical Complexity, Legacy Systems, and Dependencies

Organizational decisions occur within technical environments that may constrain the available responses. Legacy applications may depend on unsupported operating systems, proprietary software, or hardware that cannot be replaced quickly. Patching can disrupt integrations, invalidate vendor support, or introduce compatibility problems. In such circumstances, remediation may require a broader modernization project rather than a simple configuration change.

Risk management also becomes more difficult when assets, software components, and external dependencies are poorly documented. A team cannot reliably prioritize exposure if it does not know which business service depends on a vulnerable component or whether that component is accessible from the internet. Uncertain asset ownership and incomplete configuration information can undermine both risk assessment and treatment planning.

Third-party dependencies introduce additional complexity because the organization may not control the timing or technical details of a fix. A supplier may need to release a patch, a service provider may restrict configuration changes, or contractual arrangements may slow access to relevant evidence. These constraints can justify temporary deferral, but only when they are explicitly recognized and managed.

The key distinction is between a technical constraint that is documented and actively managed and one that becomes a permanent excuse for inaction. Where immediate remediation is infeasible, organizations should consider compensating controls, segmentation, access restrictions, heightened monitoring, replacement planning, and time-bound risk acceptance.

3.6 Critical Synthesis and Research Gap

The reviewed literature offers complementary explanations but also reveals a need for integration. Security economics explains why organizations may underinvest or face distorted incentives. Governance perspectives clarify the importance of authority and accountability. Behavioural theories explain why available information may be interpreted inconsistently, while technical and operational considerations explain why some treatments are difficult to execute.

 © Author(s) | CC BY 4.0 International License.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
https://ijetrm.com/

These explanations are related, not interchangeable. A lack of funding may arise from a genuine budget constraint, a weak business case, or an incentive structure that rewards other activities. An implementation delay may originate in technical dependencies or in a failure to assign ownership. The same visible outcome—an unresolved finding—can therefore arise through different mechanisms and require different interventions. The principal gap addressed by this paper is the absence, within the conceptual approach adopted here, of a unified stage-based model that connects these influences to specific decision failures, responsible actors, corrective mechanisms, and measurable outcomes. The paper responds by treating the organizational risk-response process as the unit of analysis and the individual risk-treatment decision as the focal event.

Importantly, this is a conceptual synthesis of selected literature and established guidance, not a claim that a systematic review has established the prevalence or relative strength of each barrier.

IV. THEORETICAL FRAMEWORK

Three complementary theories provide the primary explanatory foundation for the proposed model, while institutional theory helps explain the influence of external expectations.

4.1 Principal–Agent Theory

Principal–agent theory examines situations in which one party delegates responsibility to another but cannot perfectly observe or control the latter's decisions (Jensen & Meckling, 1976). In cybersecurity, this problem may arise between executives and business-unit managers, security teams and system owners, or organizations and external service providers.

A system owner may understand that a vulnerability creates enterprise risk but prefer to postpone a disruptive upgrade because the immediate performance consequences fall on the owner's department. Meanwhile, the costs of a future incident may be distributed across customers, other departments, insurers, and shareholders. The theory explains how divided authority and misaligned incentives can produce decisions that are locally attractive but organizationally harmful. It supports interventions such as explicit risk ownership, decision-rights matrices, escalation requirements, and accountability for overdue high-risk findings.

4.2 Resource-Based View

The resource-based view argues that organizational capabilities and resources influence the ability to achieve and sustain performance advantages (Barney, 1991). Applied to cybersecurity, the perspective directs attention to specialist personnel, technical infrastructure, security knowledge, financial resources, and the capacity to coordinate implementation.

An organization may approve remediation yet lack the engineers, testing environment, or vendor support required to execute it. In such cases, stronger accountability may reveal the problem but cannot independently solve it. The resource-based view therefore helps distinguish unwillingness to act from inability to act. It also suggests that cybersecurity maturity depends partly on whether the organization can mobilize its capabilities when risks are identified, rather than merely whether it possesses security tools.

4.3 Behavioural Decision Theory

Behavioural decision theory explains how uncertainty, framing, limited attention, and cognitive constraints shape decisions. Prospect theory provides a foundation for examining why decision-makers may respond inconsistently to potential losses and gains (Kahneman & Tversky, 1979), while bounded rationality emphasizes the limits of fully optimizing decisions under practical constraints (Simon, 1997).

In cybersecurity, these perspectives help explain why immediate operational disruption may receive more attention than a probabilistic future incident. They also clarify why a technically detailed report may fail to produce action when managers cannot readily interpret its business implications. This theoretical lens supports clearer risk communication, standardized decision criteria, explicit treatment deadlines, and escalation based on both severity and exposure.

4.4 Institutional Theory

Institutional theory examines how organizations respond to regulatory requirements, professional norms, and expectations for legitimacy (DiMaggio & Powell, 1983). Cybersecurity programs may be shaped by audits, certification requirements, contractual obligations, and industry standards. Such pressures can encourage better practices, but they may also produce a gap between formal compliance and operational effectiveness. An organization might maintain policies, complete required assessments, and document its risk register while repeatedly deferring difficult remediation work. Institutional theory therefore provides a contextual explanation for why visible conformity

 © Author(s) | CC BY 4.0 International License.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
https://ijetrm.com/

may not always correspond to effective risk reduction. It should not be interpreted as implying that compliance efforts are inherently superficial.

4.5 Integration of the Theories

The theories address different but interacting mechanisms. Principal–agent theory explains how authority and incentives shape decisions; the resource-based view explains whether the organization possesses the capacity to implement them; behavioural decision theory explains how decision-makers interpret uncertain risk information; and institutional theory explains the external expectations within which decisions occur.

Together, they support a central proposition: the likelihood that an identified risk will be treated effectively depends not only on the technical quality of the finding, but also on the alignment of decision authority, incentives, capabilities, and risk interpretation.

The theoretical framework does not assume that any single mechanism is universally dominant. Its purpose is to identify the mechanism operating in a particular risk-response failure and guide a proportionate intervention.

V. METHODOLOGY

5.1 Research Design

This paper adopts a conceptual, literature-based research design using an integrative approach. Integrative reviews are suitable for bringing together evidence and ideas from different research traditions to develop a broader conceptual understanding of a problem (Torraco, 2005; Snyder, 2019). The study combines literature on cybersecurity investment, organizational governance, decision-making, risk assessment, and security management standards. Its purpose is to develop an explanatory framework, rather than to estimate the statistical prevalence of unresolved risks or test causal relationships using original organizational data.

5.2 Sources and Search Approach

Relevant material for this type of study includes peer-reviewed journal articles, scholarly books, conference proceedings, official cybersecurity guidance, and recognized international standards. Suitable databases for a reproducible future search include Scopus, Web of Science, IEEE Xplore, ACM Digital Library, and ScienceDirect. Google Scholar may supplement these databases, particularly for interdisciplinary research and citation tracking.

Relevant search terms include:

- “cybersecurity risk management” AND “organizational barriers”
- “vulnerability remediation” AND “organizational factors”
- “cybersecurity investment” AND “incentives”
- “cybersecurity governance” AND “accountability”
- “risk acceptance” AND “information security”
- “cybersecurity” AND “decision-making” AND “resource constraints”
- “security patch management” AND “implementation delays”

Official publications from NIST and ISO provide normative guidance against which the academic literature can be interpreted. Such publications are not treated as equivalent to empirical studies: standards describe recommended practices, whereas empirical research examines observed relationships or outcomes.

Methodological limitation: This paper does not report a completed systematic database search, a PRISMA screening process, a verified number of included studies, or a formal study-by-study quality assessment. The sources discussed constitute a conceptual synthesis. A subsequent systematic review would need to document database-specific search strings, search dates, screening decisions, exclusion reasons, and quality-appraisal procedures before making claims about the completeness of the evidence.

5.3 Inclusion and Exclusion Principles

The synthesis prioritizes sources that explain at least one of the following: cybersecurity risk assessment, investment incentives, organizational governance, remediation decisions, human decision-making, security management capabilities, or institutional influences on cybersecurity practice.

5.4 Analytical Procedure

The literature is interpreted through four linked analytical steps.

First, relevant concepts are identified, including risk ownership, remediation cost, organizational capacity, risk communication, formal acceptance, and verification.

Second, these concepts are mapped onto the seven stages of the risk-response process developed in Section 2.

 © Author(s) | CC BY 4.0 International License.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
https://ijetrm.com/

Third, the theoretical perspectives are used to explain how particular barriers may produce observable failures. For example, fragmented authority may delay authorization, while insufficient implementation capacity may delay completion after approval.

Finally, the mechanisms are integrated into a conceptual framework linking organizational conditions to decision processes and risk-response outcomes. This framework generates propositions for future empirical testing rather than conclusions about causal effects already established by this study.

5.5 Research Quality and Limitations

The approach draws on peer-reviewed research and recognized institutional guidance, but the sources differ in purpose and evidentiary strength. Theoretical models identify possible mechanisms; qualitative case studies provide contextual explanations; quantitative studies estimate relationships under particular assumptions; and standards specify recommended practices. Their findings should not be combined as though they represented equivalent forms of evidence.

The paper's principal limitation is that it does not independently validate the proposed framework against organizational records or interview data. Its conclusions are analytical and conceptual. The framework should therefore be tested in organizations of different sizes, sectors, and levels of cybersecurity maturity before its predictive usefulness or generalizability can be established.

VI. FINDINGS AND CONCEPTUAL SYNTHESIS

The synthesis supports five interconnected explanations for why identified cybersecurity risks may remain unresolved. These are conceptual themes drawn from the literature, not measured findings about their frequency or relative importance.

6.1 Recognition Without Authority

The first mechanism arises when an organization identifies a risk but does not clearly assign the authority to decide what happens next. Security professionals may have the expertise to evaluate exposure but lack control over business budgets, application availability, or vendor contracts.

A finding can consequently remain in a register while departments debate responsibility. Escalation may also fail when there is no agreed threshold for referring overdue or high-impact risks to senior management. The appropriate intervention is to define who validates a finding, who owns the affected business risk, who authorizes treatment, and who may accept residual risk. Accountability should follow actual decision rights rather than job titles alone.

6.2 Authorization Without Resources

A second mechanism appears when a treatment plan is approved but the organization does not provide the resources needed to execute it. The decision may be reasonable in principle, yet implementation stalls because funding, staff time, testing facilities, or vendor support is unavailable. This mechanism illustrates why approval rates are insufficient measures of success. An organization may approve most remediation plans while allowing a large proportion to remain incomplete.

The corrective response should connect approval to resource commitments, named implementation teams, milestones, and an escalation process for unresolved dependencies. Where resources are genuinely unavailable, the risk owner should decide whether to fund an alternative treatment, reduce exposure temporarily, or formally accept the residual risk within authorized limits.

6.3 Resources Without Aligned Incentives

A third mechanism occurs when resources are available but other performance priorities discourage action. Teams may postpone upgrades because they are rewarded for uptime, rapid project delivery, or short-term cost control. The consequences of cybersecurity incidents, by contrast, may be uncertain or fall outside the team's immediate performance assessment. This pattern reflects the incentive problems identified in security economics and organizational theory (Anderson & Moore, 2006; Fedele & Roner, 2022). It suggests that increasing the security budget will not necessarily resolve the gap if managers continue to face conflicting performance expectations. Organizations should incorporate risk-treatment obligations into operational planning and managerial accountability. This does not mean rewarding teams solely for the number of vulnerabilities closed. It means recognizing justified prioritization, timely escalation, effective risk reduction, and responsible management of residual exposure.

6.4 Implementation Without Verification

 © Author(s) | CC BY 4.0 International License.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
https://ijetrm.com/

A fourth mechanism arises when organizations treat task completion as equivalent to risk reduction. A ticket may be marked closed after a patch is installed, a configuration is changed, or a control is deployed. Yet the original weakness may persist because the patch failed, the wrong asset was modified, the change introduced a new exposure, or the control does not address the relevant attack path. The distinction between activity and outcome is fundamental. Implementation records show that work was attempted; verification establishes whether the intended risk treatment succeeded. Verification should therefore include appropriate technical retesting, configuration checks, control-effectiveness assessment, and updates to the residual-risk record. Where relevant, the organization should reassess whether related assets or dependencies remain exposed.

6.5 Risk Acceptance Without Effective Governance

A fifth mechanism involves the informal normalization of unresolved risks. A finding may remain open for months because teams repeatedly defer it, although no authorized individual has explicitly accepted the residual exposure. Such a situation differs from legitimate risk acceptance. Acceptance requires a clear understanding of the residual risk, the reason for retaining it, the authority of the decision-maker, any mandatory constraints, and the conditions under which the decision must be reviewed. Risk acceptance should not become a permanent administrative label for work that has not been completed. Decisions should be time-bound where appropriate, supported by interim controls, and reconsidered when threat conditions, system exposure, or available treatment options change.

6.6 The Importance of Context

The five mechanisms do not operate independently. A small organization may have limited resources but short decision chains. A large organization may have specialist teams and substantial funding but suffer from fragmented authority. A highly regulated organization may have clear acceptance rules while still experiencing implementation delays because of legacy systems.

Risk characteristics also matter. Internet-facing systems, actively exploited vulnerabilities, critical business services, and risks with serious safety or legal consequences may require faster escalation than low-impact findings with effective compensating controls. Context should influence treatment decisions without becoming an excuse for ignoring high-consequence exposure.

6.7 Integrated Interpretation

The conceptual synthesis suggests that the cybersecurity design gap is best understood as a process failure rather than a single organizational deficiency. Technical identification, managerial authorization, resource allocation, implementation, and verification are connected stages. Weakness at one stage can obstruct the others, and several barriers may reinforce one another. he resulting framework treats effective risk response as the outcome of a coordinated chain: risk information must be credible, the business implications must be understood, an accountable owner must make or obtain the necessary decision, resources must support the selected treatment, and the outcome must be verified.

VII. PROPOSED INTEGRATED CONCEPTUAL FRAMEWORK

7.1 Structure of the Framework

The proposed framework links organizational conditions to the processes through which identified risks are treated. It distinguishes factors that influence decisions, the mechanisms through which those factors operate, and the outcomes that indicate effective or ineffective risk response.

Organizational conditions

Governance and accountability · managerial incentives · resources and costs · risk communication · organizational culture · technical complexity · third-party dependencies

Risk-response mechanisms

Ownership · business-risk interpretation · prioritization · authorization · funding · implementation coordination · verification

Risk-response outcomes

Timely treatment · verified risk reduction · justified deferral · accountable acceptance · reduced recurrence · fewer overdue high-risk findings

Contextual influences: organizational size, cybersecurity maturity, system criticality, regulatory obligations, exposure to exploitation, and the availability of effective compensating controls. Monitoring and reassessment feed new information back into the next decision cycle.

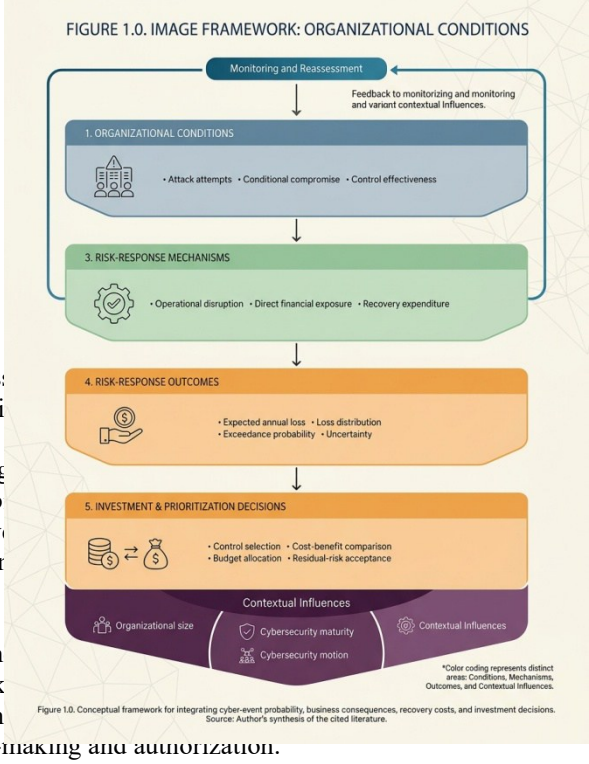
 © Author(s) | CC BY 4.0 International License.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
https://ijetrm.com/

Figure 1. Proposed conceptual framework for explaining and reducing the cybersecurity design gap. Source: Author's conceptual synthesis.

7.2 Independent Variables

The framework identifies seven broad groups of organizational conditions.



These variables should not be as nfluence depends on the type of risk, the organization's capabi unters difficulty.

7.3 Mediating Processes

The framework proposes that org ntifiable decision processes. For example, unclear accountab delays authorization. Limited funding may prevent an approv k communication may cause senior management to underestir g its priority relative to other demands.

The proposed mediators are:

1. Clarity of ownership an
2. Quality of business-risk
3. Accuracy and consisten
4. Timeliness of decision-making and authorization.
5. Availability of implementation resources.
6. Coordination of implementation activities.
7. Verification and feedback quality.

These mediating processes make the framework practically useful because each can be examined through organizational records, interviews, and observed decisions.

7.4 Dependent Variable: Risk-Response Effectiveness

Risk-response effectiveness is the extent to which an organization makes and executes an appropriate, accountable, and verifiable decision about an identified cybersecurity risk. It should be assessed through several complementary indicators:

Indicator	Operational interpretation
Time to authorization	Time between validation of a finding and the authorized treatment decision
Time to verified treatment	Time between validation and confirmation that the selected treatment is effective
Deadline compliance	Proportion of findings treated or formally reassessed within their approved deadlines
High-risk backlog	Number, severity, and age of significant unresolved findings
Ownership coverage	Proportion of material findings with an accountable owner
Acceptance quality	Proportion of accepted risks with authorized approval, documented rationale, review conditions, and appropriate safeguards
Verified risk reduction	Evidence that the selected treatment has reduced exposure or potential consequences
Recurrence rate	Frequency with which the same or related weaknesses reappear after treatment

No single indicator adequately captures performance. Mean remediation time, for instance, can improve simply because an organization closes numerous low-risk findings while leaving a smaller number of serious exposures

 © Author(s) | CC BY 4.0 International License.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
https://ijetrm.com/

unresolved. Similarly, a high closure rate may conceal weak verification. Measures should therefore be disaggregated by severity, asset criticality, exploitation status, treatment type, and relevant operational constraints. A justified deferral should not be counted automatically as failure, but neither should it be considered successful merely because it has been documented.

7.5 Moderating Variables

The relationships in the framework may vary according to organizational size, cybersecurity maturity, regulatory environment, system criticality, technical complexity, and threat exposure. For instance, clearer ownership may improve decision speed in a relatively simple organization, while a multinational enterprise may still require extensive coordination across jurisdictions and business units. Likewise, an unavailable patch may justify a different treatment pathway from an actively exploited vulnerability for which an effective fix exists. These contextual factors should be recorded when comparing organizations. Without them, apparent differences in remediation performance may reflect dissimilar risk environments rather than better or worse management.

7.6 Propositions for Future Research

The framework generates six propositions for empirical investigation.

- P1: Greater clarity of risk ownership and decision rights is associated with shorter authorization delays for identified cybersecurity risks.
- P2: Misalignment between managerial performance incentives and cybersecurity objectives is associated with a greater likelihood of unjustified remediation deferral.
- P3: Greater implementation capacity strengthens the relationship between approved treatment plans and verified completion.
- P4: Poor-quality risk information and weak communication of business consequences reduce the likelihood that technically significant risks receive appropriate management priority.
- P5: Clear escalation procedures and formal risk-acceptance requirements are associated with fewer significant risks remaining unresolved without an authorized decision.
- P6: The relationships proposed in P1–P5 vary according to organizational maturity, system criticality, technical complexity, regulatory obligations, and threat exposure.

These propositions are testable hypotheses, not established causal findings. Their relationships may differ across settings, and empirical analysis should account for confounding variables such as vulnerability severity, asset exposure, and patch availability.

VIII. A PROPOSED FRAMEWORK FOR IMPROVING RISK-RESPONSE DECISIONS

The conceptual model can be translated into a practical governance process. The purpose is not to create another administrative layer but to ensure that every significant finding progresses toward an appropriate, accountable outcome.

8.1 Establish Risk-Based Prioritization

Organizations should prioritize findings using more than a technical severity score. Relevant considerations include exploitability, evidence of active exploitation, internet exposure, asset criticality, potential business impact, existing safeguards, and the feasibility of treatment. In practice, an organization should combine technical assessment with knowledge of its own assets and operating environment.

Consider two findings rated similarly by a scanner. One affects an externally accessible system supporting a critical customer service; the other affects an isolated test system containing no sensitive information. A uniform remediation deadline may not reflect their different business implications. Conversely, a lower-rated weakness on a critical system should not automatically be dismissed if it forms part of an exploitable attack path. Prioritization should remain transparent, periodically reviewed, and subject to mandatory requirements where applicable.

8.2 Define Decision Rights and Accountability

Every material finding should have an identifiable owner and a clear decision pathway. The following division of responsibility provides a starting point.

Role	Primary responsibility
Security team	Validate findings, assess technical exposure, recommend treatment options, and define verification requirements

 © Author(s) | CC BY 4.0 International License.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
https://ijetrm.com/

Business or system owner	Explain business impact, operational constraints, and the implications of treatment
Risk owner	Account for the risk and coordinate the treatment decision
Budget holder	Approve or allocate necessary financial and personnel resources
Authorized risk authority	Approve residual-risk acceptance within delegated limits
Implementation team	Execute the treatment and document changes
Independent assurance or designated reviewer	Verify treatment effectiveness and challenge unsupported closure decisions

In smaller organizations, one individual may perform several roles. What matters is that the responsibilities remain explicit and that high-consequence risk acceptance receives an appropriate level of independent scrutiny. The person implementing a control should not automatically have unlimited authority to accept the residual risk created when that control cannot be completed.

8.3 Introduce a Structured Risk-Response Protocol

A practical protocol should require the following sequence:

1. Validate the finding and identify affected assets.
2. Translate the technical evidence into business consequences and document uncertainty.
3. Assign an accountable owner and determine the appropriate priority.
4. Evaluate feasible treatment options, including remediation, avoidance, alternative mitigation, or acceptance where permitted.
5. Authorize the selected response and commit the required resources.
6. Implement the response, document any deviations, and maintain interim safeguards when needed.
7. Verify effectiveness, reassess residual risk, and update the risk register.
8. Escalate overdue or materially changed risks for renewed decisions.

This process should be proportionate. A critical, actively exploited exposure may require immediate escalation, while a lower-impact issue may be handled through routine maintenance. The objective is consistent decision quality, not identical administrative effort for every finding.

8.4 Improve Economic Decision Support

Security teams should present decision-makers with comparable treatment options rather than a recommendation detached from business constraints.

For each material risk, the decision record should identify the expected benefits, implementation costs, operational consequences, uncertainties, available alternatives, and any mandatory requirements. A simplified decision rule can be expressed as:

$$a^* = \arg\min_{a \in \mathcal{A}} [E(L \mid a, D) + C(a)]$$

where:

- a is a candidate risk-response action.
- $\mathcal{A}$ is the set of feasible actions.
- L is the potential loss under the selected action.
- D represents the available risk evidence.
- C(a) represents the cost of implementing the action.

The expression illustrates the principle of comparing expected loss and treatment cost. It is not a complete financial model: organizations may also need to consider non-monetary consequences, legal duties, safety constraints, risk appetite, uncertainty, and dependencies between risks. Where a mandatory control or legal obligation applies, the feasible action set must reflect that constraint rather than treating noncompliance as an ordinary economic alternative.

8.5 Strengthen Escalation and Risk Acceptance

Risk acceptance should be governed by documented authority and review conditions. A record should specify the risk being accepted, the rationale, the anticipated consequences, existing safeguards, the approving authority, the review date, and events that would trigger reconsideration.

Escalation should be triggered when a risk exceeds the organization's tolerance, remains unresolved beyond an approved deadline, changes materially in severity, or becomes subject to new evidence of exploitation. An escalation should require a decision, not merely another notification.

 © Author(s) | CC BY 4.0 International License.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
https://ijetrm.com/

For example, if a supplier cannot provide a patch for a serious vulnerability, the organization may need to restrict access, isolate the affected service, introduce additional monitoring, or plan a replacement. If these measures do not reduce the risk sufficiently, an authorized leader must determine whether continued operation is acceptable under the relevant legal, contractual, and organizational constraints.

8.6 Use Automation With Human Oversight

Automation can help correlate findings with asset inventories, identify duplicate records, track deadlines, assign work, detect recurring weaknesses, and trigger escalation. It can also support continuous monitoring and help organizations recognize when previously acceptable risks require reassessment.

However, automated prioritization is only as reliable as its underlying data and decision rules. Poor asset inventories, incomplete dependency information, or inaccurate assumptions about exploitability can produce misleading priorities. Automated closure rules may also mistake a completed workflow for effective treatment. Automation should therefore support, rather than replace, accountable risk decisions. Material risks and exceptions should retain traceable decision records and appropriate human review.

8.7 Develop Organizational Capability and Learning

Sustainable improvement requires more than enforcing deadlines. Organizations need sufficient technical capacity, reliable asset information, clear escalation pathways, and a culture in which staff can report implementation barriers without concealing them.

Post-incident reviews, near-miss analysis, recurring audit findings, and remediation retrospectives can reveal weaknesses in the decision process itself. If the same class of vulnerability repeatedly returns, the underlying problem may be insecure procurement, inadequate testing, insufficient staff training, or a flawed change-management process. Learning should consequently address both the individual finding and the organizational conditions that allowed it to arise or remain unresolved.

8.8 Measure Outcomes Rather Than Administrative Activity

An effective performance dashboard should combine measures of timeliness, quality, and residual exposure. It may track the age and severity of unresolved findings, the time between identification and authorization, the time between authorization and verified treatment, overdue high-risk decisions, risk-acceptance quality, and recurring weaknesses.

Measures should be interpreted together. An organization that closes findings rapidly but experiences repeated recurrence may be optimizing the wrong outcome. One that has a longer remediation time because it is safely managing complex legacy systems may perform better than a faster organization that accepts unexamined exposure. The purpose of measurement is to improve decisions and reduce risk, not to encourage teams to manipulate closure statistics.

8.9 Phased Implementation

Implementation should begin with a baseline assessment of the organization's existing risk-response process. A practical sequence is:

- Phase 1 — Diagnose: Review a sample of unresolved findings, identify decision bottlenecks, and establish baseline indicators.
- Phase 2 — Clarify: Assign owners, define decision rights, establish escalation thresholds, and standardize risk-acceptance records.
- Phase 3 — Operationalize: Connect treatment decisions to budgets, implementation milestones, verification requirements, and management reporting.
- Phase 4 — Improve: Review performance trends, recurring weaknesses, and stakeholder feedback; revise procedures as evidence accumulates.

The framework should be adapted to organizational size, risk profile, and available resources. Smaller organizations may use a simple risk register and scheduled management review, while larger organizations may require workflow integration, automated evidence collection, and formal governance committees.

IX. DISCUSSION

9.1 Implications for Cybersecurity Theory

The proposed framework extends the analysis of cybersecurity risk by treating the conversion of risk information into effective action as a distinct organizational problem. Conventional risk management already recognizes the need for

 © Author(s) | CC BY 4.0 International License.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
https://ijetrm.com/

assessment, treatment, and monitoring. The contribution here is to connect these activities to the organizational mechanisms that may prevent them from working as intended.

Principal–agent theory explains why assigning responsibility without aligning incentives and authority may be insufficient. The resource-based view clarifies why approval does not guarantee implementation. Behavioural decision theory explains why risk information may fail to influence priorities, while institutional theory highlights the possibility that formal compliance can coexist with weak operational follow-through.

The framework brings these explanations together without suggesting that one theory can account for every unresolved risk. A failure to patch a legacy application may arise from technical incompatibility, insufficient funding, weak accountability, or a combination of these conditions. The correct explanation must be established from evidence about the specific decision process.

9.2 Implications for Management Practice

The practical implication is that cybersecurity leaders should investigate why a finding remains unresolved before prescribing a corrective measure. Increasing the number of security tools may not help when the actual barrier is a lack of decision authority. Additional training may have little effect when a department lacks the budget to implement an approved control. Management reviews should therefore examine the status of significant risks alongside the reasons for delay, the responsible decision-maker, the resources committed, the interim safeguards in place, and the evidence required to verify treatment.

This approach also changes the purpose of executive reporting. Rather than presenting a long list of technical findings, security leaders can communicate which decisions are outstanding, what consequences may follow, what options are available, and what authority or resources are required.

9.3 Economic and Regulatory Implications

The framework reinforces the need to distinguish economically justified treatment decisions from organizationally convenient postponement. Remediation costs and operational disruption are legitimate considerations, but they should be evaluated against the potential consequences of leaving a risk unresolved. A decision may be financially reasonable under one set of assumptions and unacceptable under another. Changes in threat activity, asset exposure, legal obligations, or available safeguards can alter the appropriate response. Risk acceptance must therefore be revisited when its underlying assumptions change.

Regulators and auditors can also benefit from examining decision quality rather than relying exclusively on evidence that policies, assessments, and risk registers exist. Useful evidence includes documented ownership, approved treatment plans, justified exceptions, verified controls, and timely escalation of significant exposures.

9.4 Implications for Organizational Resilience

The proposed framework treats resilience as the ability to recognize, prioritize, and respond to changing exposure, not merely the possession of preventive technologies. Organizations that learn from delayed remediation, recurring weaknesses, and failed treatments can improve the processes that produce those outcomes. This is particularly important where systems are interconnected. A risk that appears manageable within one department may create wider exposure through shared infrastructure, software dependencies, or external suppliers. Effective governance must therefore connect local decisions with enterprise-wide consequences.

9.5 Validation and Future Research

Future research should test the framework using organizational data rather than relying on conceptual reasoning alone. A multi-case study could compare organizations that differ in size, sector, regulatory environment, and cybersecurity maturity. Interviews with security leaders, system owners, executives, and implementation teams could help identify how decisions are made and where responsibility becomes fragmented.

Longitudinal data would be particularly useful because the framework distinguishes the time required to authorize treatment from the time required to implement and verify it. Researchers could examine whether clear ownership predicts faster authorization, whether resource availability predicts completion, and whether formal acceptance procedures reduce the number of high-risk findings that remain unresolved without approval.

Quantitative studies should control for severity, exploitability, asset criticality, patch availability, operational constraints, and exposure to active threats. Otherwise, organizations managing more complex or consequential systems could appear less effective simply because their risk environments are more difficult.

 © Author(s) | CC BY 4.0 International License.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
https://ijetrm.com/

A further research direction is the development of a validated risk-response effectiveness scale. Such a measure should capture timeliness, decision quality, implementation, residual-risk reduction, and recurrence without collapsing these distinct dimensions into a single unqualified score.

IX. CONCLUSION AND RECOMMENDATIONS

10.1 Conclusion

The cybersecurity design gap describes a failure in the organizational arrangements through which identified risks are converted into appropriate and effective action. It is not synonymous with the existence of a vulnerability, nor does every unresolved finding indicate negligence. Risks may legitimately remain open when treatment is infeasible, an alternative control is effective, or an authorized decision-maker accepts the residual exposure under appropriate conditions.

The problem arises when risks remain unresolved without a defensible decision, adequate safeguards, sufficient resources, or verification that the selected response has worked. Such failures may emerge from fragmented authority, misaligned incentives, limited resources, poor risk communication, technical dependencies, or weaknesses in organizational learning.

The proposed conceptual framework integrates these factors through a stage-based model connecting organizational conditions, risk-response mechanisms, and measurable outcomes. Its central argument is that risk identification and effective treatment are separate organizational achievements. The first generates knowledge of exposure; the second requires governance, judgment, resources, implementation, and verification.

The framework is a basis for further investigation, not a validated prediction model. Its practical and theoretical value will depend on subsequent empirical testing across different organizational contexts.

10.2 Recommendations

Based on the analysis, the following recommendations are proposed:

1) Make risk ownership explicit. Assign accountable owners and clarify who may authorize treatment, commit resources, and accept residual risk.
2) Connect security priorities to business consequences. Translate technical findings into operational, financial, legal, and reputational implications.
3) Link approved decisions to resources. Ensure that remediation plans include funding, implementation responsibility, milestones, and verification criteria.
4) Align incentives with effective risk management. Avoid performance systems that reward short-term delivery while encouraging unjustified security deferrals.
5) Formalize risk acceptance and escalation. Require documented authority, rationale, safeguards, review dates, and escalation of significant overdue risks.
6) Verify treatment effectiveness. Do not equate ticket closure or control deployment with demonstrated risk reduction.
7) Measure outcomes comprehensively. Track remediation timelines, high-risk backlog, acceptance quality, verified risk reduction, and recurrence.
8) Use automation responsibly. Automate tracking and evidence collection while retaining appropriate human oversight of material decisions.
9) Institutionalize learning. Use incidents, near misses, recurring findings, and failed treatments to improve the organizational processes behind cybersecurity decisions.
10) Validate the framework empirically. Test its propositions using interviews, case studies, remediation records, and longitudinal organizational data.

Ultimately, organizations should not measure cybersecurity maturity only by how effectively they discover weaknesses. They should also assess whether they can make sound decisions about those weaknesses, mobilize the resources to address them, and demonstrate that the chosen responses have reduced risk to an acceptable level.

 © Author(s) | CC BY 4.0 International License.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
https://ijetrm.com/

REFERENCES

1) Anderson, R., & Moore, T. (2006). The economics of information security. Science, 314(5799), 610–613. https://doi.org/10.1126/science.1130992
2) Barney, J. (1991). Firm resources and sustained competitive advantage. Journal of Management, 17(1), 99–120. https://doi.org/10.1177/014920639101700108
3) DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. American Sociological Review, 48(2), 147–160. https://doi.org/10.2307/2095101
4) Fedele, A., & Roner, C. (2022). Dangerous games: A literature review on cybersecurity investments. Journal of Economic Surveys, 36(1), 157–187. https://doi.org/10.1111/joes.12456
5) Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. ACM Transactions on Information and System Security, 5(4), 438–457. https://doi.org/10.1145/581271.581274
6) International Organization for Standardization. (2022). ISO/IEC 27001:2022: Information security, cybersecurity and privacy protection—Information security management systems—Requirements. https://www.iso.org/standard/27001.html
7) Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. Journal of Financial Economics, 3(4), 305–360. https://doi.org/10.1016/0304-405X(76)90026-X
8) Joint Task Force. (2018). Risk management framework for information systems and organizations: A system life cycle approach for security and privacy (NIST Special Publication 800-37, Rev. 2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-37r2
9) Joint Task Force Transformation Initiative. (2012). Guide for conducting risk assessments (NIST Special Publication 800-30, Rev. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-30r1
10) Kahneman, D., & Tversky, A. (1979). Prospect theory: An analysis of decision under risk. Econometrica, 47(2), 263–291. https://doi.org/10.2307/1914185
11) National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST Cybersecurity White Paper 29). U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.29
12) Niesten, E., et al. (2021). Understanding incentives for cybersecurity investments: Development and application of a typology. Digital Business, 1(2), Article 100014. https://doi.org/10.1016/j.digbus.2021.100014
13) Pascoe, C., Quinn, S., & Scarfone, K. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST Cybersecurity White Paper 29). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29
14) Ross, R. (2020). Security and privacy controls for information systems and organizations (NIST Special Publication 800-53, Rev. 5). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r5
15) Ross, R., McEvilley, M., & Oren, J. (2022). Systems security engineering: Considerations for a multidisciplinary approach in the engineering of trustworthy secure systems (NIST Special Publication 800-160, Vol. 1, Rev. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-160v1r1
16) Simon, H. A. (1997). Administrative behavior: A study of decision-making processes in administrative organizations (4th ed.). Free Press.
17) Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. Journal of Business Research, 104, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039
18) Torraco, R. J. (2005). Writing integrative literature reviews: Guidelines and examples. Human Resource Development Review, 4(3), 356–367. https://doi.org/10.1177/1534484305278283

 © Author(s) | CC BY 4.0 International License.