Machine Translated by Google
RCMOS – Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.2 2026 | Submission: 08/14/2026 | Accepted: 09/10/2026 | Publication: 10/24/2026

Cybersecurity governance as a responsibility of senior management in small and medium-sized enterprises.

Cybersecurity governance as a responsibility of top management in small and medium-sized enterprises

Cybersecurity governance as senior management responsibility in small and medium-sized companies

Eduardo Henrique Bergel Cosenza Junior
Bachelor of Laws. MBA in Health Law and Hospital Compliance. Technical training in real estate transactions. Lawyer registered with the Brazilian Bar Association (OAB).

SUMMARY

This article examines the theoretical and normative foundations that support the attribution of cybersecurity to senior management, with an emphasis on small and medium-sized enterprises. It starts from the observation that the growing dependence on data, systems, and technology vendors has transformed cyber risk into business risk, with effects on operational continuity, reputation, and financial results. The research adopts a qualitative approach, exploratory and descriptive in nature, conducted through a narrative literature review with elements of integrative review and document analysis of technical standards, reference frameworks, and legislation. The framework articulates the literature on information security governance, agency theory, upper echelons theory, the economics of information security, studies on compliance behavior, organizational accident theory, and high-reliability organization theory, in dialogue with the ISO/IEC 27000 family, the NIST Cybersecurity Framework 2.0, the General Data Protection Law, and the regulations of the National Data Protection Authority. The results indicate that cybersecurity is part of the due diligence duty of administrators and that its effectiveness depends on governance decisions regarding investment, culture, third-party management, and incident preparedness. It is concluded that small and medium-sized enterprises can exercise this responsibility through measures proportionate to their size, provided that the issue is directly addressed by their management.

Keywords: cybersecurity; corporate governance; senior management; risk management; data protection.

ABSTRACT

This article examines the theoretical and regulatory foundations for assigning cybersecurity to top management, with emphasis on small and medium-sized enterprises. It starts from the observation that growing dependence on data, systems and technology suppliers has turned cyber risk into business risk, with effects on operational continuity, reputation and financial performance. The research adopts a qualitative, exploratory and descriptive approach, carried out through a narrative literature review with elements of integrative review and through documentary analysis of technical standards, reference frameworks and legislation. The theoretical framework combines the literature on information security governance, agency theory, higher echelons theory, the economics of information security, studies on compliance behavior, the theory of organizational accidents and the theory of high reliability organizations, in dialogue with the ISO/IEC 27000 family, the NIST Cybersecurity Framework 2.0, the Brazilian General Data Protection Law and the regulations of the Brazilian National Data Protection Authority. The results indicate that cybersecurity is part of the directors' duty of care and that its effectiveness depends on governance decisions regarding investment, culture, third-party management and incident preparedness. The study concludes that small and medium-sized enterprises can fulfill this responsibility through measures proportionate to their size, provided that their leaders take direct ownership of the issue.

Keywords: cybersecurity; corporate governance; top management; risk management; date

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google
RCMOS – Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.2 2026 | Submission: 08/14/2026 | Accepted: 09/10/2026 | Publication: 10/24/2026

protection.

1 INTRODUCTION

For much of the last few decades, information security has been treated in organizations as
The responsibility of the technology sector, delegated to technicians and measured by the acquisition of equipment and protection programs. This understanding has become insufficient as data, systems and
Digital services have come to underpin virtually all business activities, from revenue...
to the relationship with clients. Von Solms and Van Niekerk (2013) observed that cybersecurity
It goes beyond the protection of information in the strict sense, as it involves the protection of people, assets and interests that can be targeted through cyberspace. When an attack disrupts the
If an operation exposes customer data or compromises a company's reputation, the problem ceases to exist.
It goes from being technical to being strategic, directly impacting the decision-making sphere of those who manage the... business.
The shift is visible in the most recent normative frameworks. Version 2.0 of Cybersecurity
The framework, published by the National Institute of Standards and Technology in 2024, added to
traditional functions of identifying, protecting, detecting, responding, and recovering a new function
called governing, focused on establishing strategy, responsibilities and...
Cyber risk oversight by leadership (NATIONAL INSTITUTE OF STANDARDS AND
TECHNOLOGY, 2024). In the European Union, Directive (EU) 2022/2555 now requires that
governing bodies of essential and important entities approve cybersecurity risk management measures, supervise their implementation, and attend specific training (UNION).
EUROPEAN, 2022). In Brazil, the General Data Protection Law imposed on data agents...
handling security duties, incident reporting, and governance, with sanctions that
They can account for a significant portion of revenue (BRAZIL, 2018).
Small and medium-sized enterprises occupy a particular position in this scenario. They have fewer resources and
They have leaner technical structures, but they handle personal data and depend on suppliers of...
Technology and are subject to the same threats that affect large organizations. The objective of this
This article examines, in light of the literature on management, governance, and compliance, the...
theoretical foundations that support assigning cybersecurity responsibility to senior management, with
Special attention should be given to smaller companies. The aim is to understand why cyber risk should...
to be treated as a business risk and what governance mechanisms, third-party due diligence and
Incident response procedures allow the manager to exercise this responsibility. Following the methodology,
Six sections develop the theme, followed by final considerations.

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google

Year VII, v.2 2026 | Submission: 08/14/2026 | Accepted: 09/10/2026 | Publication: 10/24/2026

2 METHODOLOGY

The research has a qualitative approach and a theoretical-conceptual character, with exploratory and...
descriptive. According to Gil (2017), exploratory research allows for greater familiarity with a
problem and formulate propositions about it, whereas descriptive research deals with
Characterization of phenomena and the relationships between them. The phenomenon examined here is displacement.
From cybersecurity in the technical field to the field of corporate governance, and the relationships
The analyses involve this shift, the organizational theories that explain it, and the instruments.
regulations that give it substance.

The central procedure was a narrative literature review, with elements of an integrative review.
Snyder (2019) indicates that these modalities are appropriate when the intention is to monitor the
developing a field of research, articulating contributions from different disciplines, and proposing
Conceptual syntheses, without the intention of statistically aggregating empirical results. Torraco
(2005) adds that the integrative review allows gathering and critiquing representative literature on a
the theme in order to generate new perspectives, a characteristic pertinent to an object situated at the intersection
between information systems, administration, economics and law.

The selection of the corpus was based on widely recognized works on security governance.
information, such as that of Von Solms and Von Solms (2004) and Posthumus and Von Solms (2004), about
security economics, such as those by Anderson (2001) and Gordon and Loeb (2002), and about
conformity behavior, such as those of Bulgurcu, Cavusoglu and Benbasat (2010) and Siponen and
Vance (2010). Based on these works, a search was conducted for related published studies.
in peer-reviewed journals such as MIS Quarterly, Information Systems Research, Computers
& Security and Journal of Information Systems. The inclusion criteria were direct relevance to
The topic, its recognized relevance in the literature, and the possibility of fully verifying the source.

In addition, a documentary analysis of technical standards and reference frameworks was carried out.
and legislation. ABNT NBR ISO/IEC 27001:2022 and ABNT NBR ISO/IEC were examined.
27002:2022, ISO/IEC 27014:2020, ABNT NBR ISO 31000:2018, NIST Cybersecurity
Framework 2.0 and the NIST SP 800-161 Rev. 1 and NIST SP 800-61 Rev. 3 publications, in addition to Law No.
13.709/2018, of the resolutions of the National Data Protection Authority on small data agents.
Regarding the reporting and communication of incidents, Law No. 6.404/1976, the Civil Code, and Decree No.
11.856/2023 and Directive (EU) 2022/2555. To illustrate the economic dimension of the problem,
Data published in IBM's annual Cost of a Data Breach reports and in Data Breach were used.
Investigations Report, from Verizon.

The material was organized by thematic categorization into six axes, corresponding to the sections of

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google

Year VII, v.2 2026 | Submission: 08/14/2026 | Accepted: 09/10/2026 | Publication: 10/24/2026

development of the article. It is acknowledged as a limitation its exclusively theoretical nature and documentary evidence of the investigation, as well as the fact that the sectoral reports used are based on Our own samples, not necessarily representative of small Brazilian businesses.
For this reason, quantitative data are used only to illustrate the magnitude of
The phenomenon, and the propositions formulated, must be verified in future empirical research.

3. From Information Security to Cyber Governance

The literature on information security has followed a path that goes from technical concerns to... organizational concern. Dhillon and Backhouse (2001), when reviewing research trends then existing, they argued that the prevailing approach, centered on technical controls and on Formal access models were insufficient to deal with problems that originated in Social structures, norms, and responsibilities within organizations. The authors argue a socio-organizational perspective, in which security is understood as a result of interaction between people, processes, and technology, and not just as a property of systems. computational. This shift in focus opened up space for management and, subsequently, the governance would then take center stage in the debate.
Von Solms and Von Solms (2004) contributed to this transition by identifying ten recurring errors. in information security management, among which is the perception that security is a problem. exclusively technical, the absence of involvement from senior management, the lack of formal policies and the lack of monitoring and compliance mechanisms. The authors proposed that these elements were used by management as a checklist to assess the completeness of a security governance plan. Posthumus and Von Solms (2004), in the same year, presented an information security governance model that situates the topic within the framework of governance. corporate, under the responsibility of the board and senior management, and which incorporates considerations technical requirements meet business, legal, and regulatory demands.
Schneier (2000) summarized the spirit of this evolution by stating that security is a process, not... a product. The acquisition of technological tools, however sophisticated they may be, does not replace a product. Defining objectives, assigning responsibilities, continuous monitoring, and review. periodic controls. Soomro, Shah and Ahmed (2016), in a literature review on the role of In the field of information security management, they concluded that the literature converged on the need for a a holistic approach, in which managerial activities, such as policy development, allocation Regarding resources, awareness, and alignment with strategy, they receive the same attention as... Technical aspects are now treated as part of the managers' responsibility.

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google

Year VII, v.2 2026 | Submission: 08/14/2026 | Accepted: 09/10/2026 | Publication: 10/24/2026

The normative frameworks have followed this trend. ISO/IEC 27014:2020 addresses this.
specifically regarding information security governance and structuring the agency's actions.
governance in evaluation, direction, monitoring, and communication processes, distinguishing them from
management activities (INTERNATIONAL ORGANIZATION FOR STANDARDIZATION;
INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2020). ABNT NBR ISO/IEC
Regulation (EC) 27001:2022, which establishes the requirements for an information security management system, requires
that senior management demonstrate leadership and commitment, ensuring that the policy and objectives
security measures must be compatible with the organization's strategic direction and the necessary resources must
be available (Brazilian Association of Technical Standards, 2022a).
The inclusion of the governing function in the NIST Cybersecurity Framework 2.0 represents the most significant step forward.
recent developments in this trajectory. The role encompasses the organizational context, the risk management strategy,
the roles, responsibilities and authorities, the policy, supervision and risk management of the supply chain
cyber supplies, and it is presented as an element that informs how the organization
performs other functions (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY,
(2024). In Brazil, Decree No. 11,856/2023 established the National Cybersecurity Policy and the
National Cybersecurity Committee, signaling the incorporation of the topic into the public agenda (BRAZIL,
2023). This set of references indicates that cybersecurity has come to be understood
as a dimension of corporate governance, the direction of which falls to those responsible for the fate of the
organization.

4. The Responsibility of Directors Under Agency Theories AND FROM THE HIGHER RANKS

Agency theory offers a first foundation for understanding why security
Cybernetics cannot be entirely delegated. Jensen and Meckling (1976) defined the relationship of
An agency is defined as one in which the principal delegates to the agent the performance of activities on their behalf, and
They demonstrated that the divergence of interests and the asymmetry of information between them generate costs.
monitoring, guarantee and residual loss. When the owner or manager delegates the
To ensure the safety of an internal team or an external provider, this is precisely the type of...
The agent possesses technical information that the principal does not, and their incentives are not equal.
They always coincide with those of the organization, since the cost of a failure falls primarily on the company.
and their data subjects.

Eisenhardt (1989) argued that the efficiency of agency contracts depends, among other factors,
the existence of information systems capable of making the agent's behavior observable.

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google
RCMOS - Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.2 2026 | Submission: 08/14/2026 | Accepted: 09/10/2026 | Publication: 10/24/2026

In the field of cybersecurity, these systems correspond to maturity indicators.
Periodic reports, audits, and incident response tests. Without them, the manager has no way to...
to assess whether the delegated security is being effectively exercised, and the absence of apparent incidents.
This can be confused with adequate protection. The agency literature therefore suggests that the
The involvement of senior management does not replace technical competence, but it is a prerequisite for...
Delegation must be controlled so that agency costs remain at an acceptable level.
The theory of upper echelons, formulated by Hambrick and Mason (1984), adds a second
This perspective argues that organizational results reflect, in part, the characteristics of the
The experiences and values of senior management members. Empirical studies have applied this theory.
to cybersecurity. Kwon et al. (2013) examined the association between the involvement of
Technology executives in senior management, their compensation structure, and the occurrence of violations.
information security. Haislip, Lim and Pinsker (2021), based on reported breaches between
In 2005 and 2017, it was found that CEOs with knowledge in information technology...
and the presence of the chief technology executive on the senior management team were associated with lower
The occurrence of violations led to the conclusion that the risk is a shared responsibility of the leadership.
Brazilian law offers a third foundation, of a normative nature. Law No.
Law 6.404/1976, in its article 153, determines that the company's administrator must employ, in the exercise of
their duties, the care and diligence that every active and honest man usually employs in
managing their own affairs, and article 158 deals with their liability for damages.
caused when acting with negligence or intent or in violation of the law or statute (BRAZIL, 1976).
Article 1011 of the Civil Code reiterates the duty of care and diligence for administrators of
societies in general (BRAZIL, 2002). In an environment where dependence on systems and data is
Given the intensity of the threats, which are widely known, ignoring cyber risks is hardly an option.
It is compatible with this pattern of conduct.
The LGPD reinforces this interpretation by requiring data processing agents to adopt security measures,
technical and administrative measures capable of protecting personal data from unauthorized access and
accidental or unlawful situations, as defined in article 46, and by providing, in article 50, the possibility of
formulation of rules of good practices and governance (BRAZIL, 2018). Among the sanctions
Among the administrative penalties stipulated in article 52, there is a simple fine of up to two percent of the company's revenue.
legal entity in Brazil in the last fiscal year, limited to fifty million reais per infraction, whose
The application was governed by the dosimetry regulation of the National Data Protection Authority (AUTORIDADE
NACIONAL DE PROTEÇÃO DE DADOS, 2023). The combination between
duty of care, regulatory requirements, and empirical evidence support the conclusion that the
Cybersecurity is at the core of a manager's responsibilities.

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google
RCMOS - Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.2 2026 | Submission: 08/14/2026 | Accepted: 09/10/2026 | Publication: 10/24/2026

5. The Economics of Security and the Measurement of Cyber Risk

The economics of information security has established itself as a field of research since...
the finding that many security failures stem from misaligned incentives, and not from
technological deficiencies. Anderson (2001) argued that systems frequently fail because
The people who could protect them are not the ones who bear the consequences of their failure.
This phenomenon brings security closer to the classic problems of externalities and moral hazard.
Anderson and Moore (2006), in an article published in the journal Science, expanded on this analysis and
They showed that concepts such as network externalities, information asymmetry, and adverse selection...
They explain a significant part of the difficulties faced by organizations and markets in protecting...
your systems.

Gordon and Loeb (2002) proposed an economic model for defining the optimal level of
Investment in information security. Starting from the relationship between information vulnerability,
Regarding the probability of violations occurring and the potential loss, the authors demonstrated that, for
For certain classes of probability functions, the optimal investment does not exceed approximately 37
percent, or one over Euler's number, of the expected loss. More than the numerical value, whose
While the generality of the model has been discussed by subsequent studies, its contribution lies in demonstrating that
Investment in security should be decided based on the value of the information being protected and on...
Risk reduction achieved, which is, by definition, a management decision.
Measuring cyber risk in financial terms is a prerequisite for making this decision.
taken with foundation. Freund and Jones (2015) presented the Factor Analysis model of
Information Risk, which breaks down risk into frequency of loss events and magnitude of losses,
allowing it to be expressed in monetary values comparable to the organization's other risks.
Hubbard and Seiersen (2016) criticized the widespread use of qualitative matrices, which classify
Risks were classified as low, medium, or high, and they advocated for quantitative methods that allow for comparison.
investment alternatives. These proposals are in line with ABNT NBR ISO 31000:2018, which
It is recommended that risk analysis consider the probability of events and the magnitude of their consequences
(Brazilian Association of Technical Standards, 2018).
The economic effects of the violations have been documented by event studies and surveys.
sectoral. Cavusoglu, Mishra and Raghunathan (2004) found that companies that advertised
Security breaches lost an average of 2.1 percent of their market value over the two days.
following the announcement. IBM's annual reports, conducted with the Ponemon Institute, estimate the
The average global cost of a data breach and allow you to track its evolution, according to...

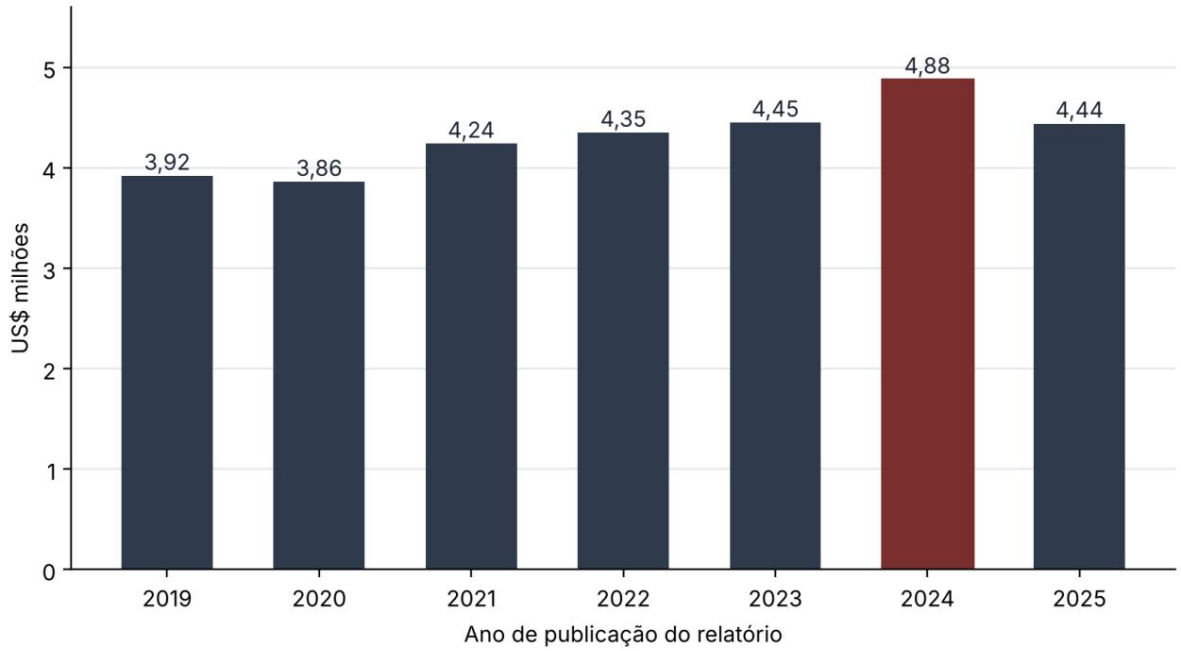
This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google
RCMOS – Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.2 2026 | Submission: 08/14/2026 | Accepted: 09/10/2026 | Publication: 10/24/2026

Figure 1 shows that the average value increased from $3.92 million in the 2019 report to $4.88 million.
millions in the 2024 report, the highest in the series, and fell to 4.44 million in the 2025 report.
reduction attributed to the greater speed in identifying and containing incidents (IBM, 2019; 2024;
2025).

Figure 1 – Average global cost of a data breach per year of publication of the report.
(US$ millions)



Source: compiled by the author with data from IBM (2019; 2020; 2021; 2022; 2023; 2024; 2025).

For the Brazilian context, the 2025 report estimated the average cost of a violation at 7.19.
millions of reais, compared to 6.75 million in the previous year (IBM, 2025). These values are derived from samples.
specific to research, composed of organizations of different sizes and sectors, and should not be
These figures are passed directly to small businesses, but they indicate the magnitude of the losses.
involved, encompassing detection, containment, notification, business loss and post-response.
incident. The reduction observed in 2025, associated by the research itself with the improvement in capacity
Detection and containment suggests that management decisions regarding preparedness and response affect...
directly impacts the final cost of incidents, which reinforces the argument that the issue should be addressed.
as an economic and strategic issue, and not just an operational one.

6. The Human Factor and the Culture of Conformity

The human dimension occupies a central position in cybersecurity. Data Breach Investigations

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google
RCMOS – Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.2 2026 | Submission: 08/14/2026 | Accepted: 09/10/2026 | Publication: 10/24/2026

2024 report, compiled by Verizon based on the analysis of thousands of incidents and violations.
Confirmed cases indicated that 68 percent of the breaches involved a non-malicious human element.
such as errors or manipulation through social engineering, and that 32 percent involved some technique.
extortion, including ransomware (VERIZON, 2024). This data reinforces the perception that
Technological controls, while indispensable, are insufficient when the people operating them...
The systems are unaware of the risks or do not feel responsible for preventing them. According to the manager, this data...
This indicates that investing in people and processes is just as important as investing in...
technology, and that the company's exposure depends directly on working conditions and
information provided to its employees.

Research in information systems has devoted extensive attention to the factors that explain the
compliance with safety policies by employees. Bulgurcu, Cavusoglu and Benbasat (2010)
They demonstrated that the intention to comply with these policies is influenced by the employee's attitude.
by normative beliefs and self-efficacy, and that attitude, in turn, is shaped by beliefs about
the benefits and costs of compliance and non-compliance, about which awareness in
Information security exerts a significant influence. Herath and Rao (2009) found that pressures
social factors, the certainty of detection, and the perception that one's own behavior contributes to the
security is associated with intentions that are more favorable to policy compliance, while
The severity of the punishments was contrary to what was expected from purely ethical approaches.
deterrents, a negative effect on these intentions.

The deterrence-based approach has received specific attention. D'Arcy, Hovav and Galletta (2009)
They found that users were aware of the existence of security policies,
Computer awareness and monitoring programs are associated with the perception of
The severity of the sanctions and, through them, the reduction of the intention to misuse the systems. Siponen
Vance (2010), in turn, showed that employees resort to neutralization techniques, such as
the denial of harm or the invocation of higher loyalties to justify policy violations, and
that these rationalizations can reduce the effect of sanctions. The combination of these results indicates
Rules and punishments have a limited effect if they are not accompanied by a clear explanation.
Regarding the reasons for the controls.

Reason's (1997) theory of organizational accidents offers a useful framework for interpreting
These findings. The author distinguished between active failures, committed by those on the front lines, and...
latent conditions, created by design, management and resource allocation decisions, that
They remain dormant in the system until they combine with active faults to produce a
accident. Applied to cybersecurity, this distinction suggests that an employee's click on
A fraudulent message is often simply the active flaw revealing latent conditions.

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google
RCMOS - Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.2 2026 | Submission: 08/14/2026 | Accepted: 09/10/2026 | Publication: 10/24/2026

previous issues, such as lack of training, excessive permissions, lack of multifactor authentication, or Lack of procedures to verify unusual payment requests.

For senior management, the main implication is that safety culture is a product of choices. managerial. ABNT NBR ISO/IEC 27002:2022 includes, among the controls related to people, the awareness, education and training in information security, terms and conditions of employment and the disciplinary process (Brazilian Association of Technical Standards, 2022b). Directive (EU) 2022/2555 goes further and requires that the members of the bodies themselves Management receive training, and similar training should be offered regularly to employees (EUROPEAN UNION, 2022). The example of leadership, consistency between discourse and resource allocation, and the willingness to listen and correct mistakes without looking for someone to blame. Individuals are elements that the literature associates with the formation of an effective culture of conformity.

7. THIRD PARTIES, SUPPLY CHAIN AND CYBER DUE DILIGENCE

Dependence on technology vendors has become a structural characteristic of companies. contemporary companies, especially smaller ones, that rely on cloud services and systems of Management contracted as a service, payment providers, and technical support providers. Each One of these relationships expands the organization's attack surface. Data Breach Investigations The 2024 report recorded that 15 percent of the violations analyzed involved a third party, such as data custodians or software vendors, which represented a 68 percent increase in in relation to the previous period (VERIZON, 2024). The company's security becomes dependent, to a greater extent, on the company's security. a considerable portion of the practices of those she hires, which transforms the selection and monitoring of Suppliers in risk management decision-making.

Transaction cost economics helps to understand why this dependence requires governance. specifically. Williamson (1985) demonstrated that transactions characterized by specific assets, Uncertainty and the limited rationality of the parties demand more elaborate governance structures. that is not simply a market exchange. Technology contracts exhibit these characteristics with intensity, as it involves company data stored in third-party systems and integrations. difficult to replace and technical information that the client rarely gets to assess. A Information asymmetry, in this context, favors the selection of suppliers with best practices. deficient, since the quality of the security offered is not directly observable at the time of hiring.

Cyber due diligence of suppliers is the organizational response to this problem. (ABNT) NBR ISO/IEC 27002:2022 dedicates a set of controls to supplier relationships, which

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google
RCMOS - Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.2 2026 | Submission: 08/14/2026 | Accepted: 09/10/2026 | Publication: 10/24/2026

It encompasses information security in these relationships, the handling of security in agreements with suppliers, security management in the information technology supply chain and communication, monitoring and change management in the services provided, and security in the use of cloud services (Brazilian Association of Technical Standards, 2022b). A NIST publication SP 800-161 Rev. 1 details supply chain risk management practices. cybersecurity and recommends that the depth of assessments be proportional to the criticality of the supplier and the service provided (BOYENS et al., 2022).

The LGPD (Brazilian General Data Protection Law) gives this due diligence a direct legal dimension. Article 39 stipulates that the operator... Carry out the treatment according to the instructions provided by the controller, who will verify compliance. from the instructions themselves and the rules on the matter, and article 42 establishes hypotheses of joint liability between controllers and operators for damages caused by processing of personal data (BRAZIL, 2018). In practice, the company that contracts a system of management, a storage service, or a customer service provider continues to be responsible for data from their clients, which makes it essential to know the supplier's practices and establish, The contract should include clear obligations regarding security, confidentiality, incident reporting, and auditing. and the return or deletion of data upon termination of the relationship.

For small and medium-sized enterprises, the application of these benchmarks requires proportionality. It is not While it is feasible to subject all suppliers to exhaustive evaluations, it is possible to classify them according to... their access to personal data and critical systems, and focusing due diligence on the most critical cases. Risk. Standardized questionnaires, verification of recognized certifications, contractual clauses of safety, forecasting of deadlines for incident reporting, and periodic reassessments comprise an accessible set of measures. The NIST Cybersecurity Framework 2.0, by incorporating the management of Supply chain risks in the governance function indicate that the choice and supervision of partners Technological decisions belong to leadership, not just to the purchasing or technology departments. (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2024).

8. Incident Response, Organizational Resilience, and Duties REGULATORY

The literature and technical references are based on the premise that no organization is immune to incidents, which shifts some of the attention from prevention to response capacity. The publication NIST SP 800-61 Rev. 3, 2025, reorganized the incident response recommendations in light of Cybersecurity Framework 2.0 and began treating it as an integral part of risk management. cybersecurity, linking preparedness, detection, response, and recovery activities to functions.

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google
RCMOS - Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.2 2026 | Submission: 08/14/2026 | Accepted: 09/10/2026 | Publication: 10/24/2026

from this framework, including the function of governing, and not as an isolated activity of the technical area.
(NELSON et al., 2025). This integration implies that decisions about roles, communication, resources and
recovery priorities should be established before the incident and with leadership involvement,
will be responsible for the operational, financial, and reputational consequences of the event.
The theory of high-reliability organizations provides a foundation for this preparation. Weick and
Sutcliffe (2007) identified five principles present in organizations that operate in environments
high risk with a low incidence of serious failures, concern about failures, reluctance to
simplifying interpretations, sensitivity to operations, commitment to resilience and...
deference to technical competence. The authors argued that these organizations treat small
Deviations, seen as signs of larger problems, should be avoided through simplistic explanations, and efforts should be made to contain them.
and recover from unexpected events. Transposed to cybersecurity, these principles
They suggest recording and analyzing near misses, conducting simulation exercises, and defining...
prior knowledge of who has the authority to decide in a crisis situation.
Regulatory obligations lend urgency to this preparation. Article 48 of the LGPD (Brazilian General Data Protection Law) stipulates that...
The controller shall notify the National Data Protection Authority and the data subject of the occurrence of
A security incident that may cause significant risk or damage (BRAZIL, 2018). Resolution
Brazilian Data Protection Authority (ANPD) Resolution No. 15/2024 regulated this duty and established that the communication must be carried out in
up to three business days, counted from the time the controller becomes aware that the incident has affected data.
personal, in addition to defining criteria to characterize the relevant risk or harm, such as involvement
sensitive data, data of children, adolescents or the elderly, financial data, data of
authentication or large-scale data (NATIONAL AUTHORITY FOR THE PROTECTION OF
(DATA, 2024). Meeting this deadline is hardly achievable without procedures.
previously defined.
Brazilian regulations, however, recognize the particularities of smaller companies.
Resolution CD/ANPD No. 2/2022 established differentiated and simplified treatment for agents of
small-scale treatment, with flexibility in some obligations and deadlines (AUTHORITY)
NATIONAL DATA PROTECTION LAW, 2022), and Resolution CD/ANPD No. 15/2024 determined
that incident reporting deadlines be doubled for these agents (NATIONAL DATA PROTECTION AUTHORITY, 2024).
The authority itself published
A guidance document on information security aimed at these agents, with recommendations for measures.
administrative and technical aspects, such as the adoption of information security policies and awareness campaigns.
and employee training, contract management, access control, protection of stored data and vulnerability management
(NATIONAL DATA PROTECTION AUTHORITY)
(DATA, 2021). However, this flexibility does not eliminate the duty of security, it only adapts its

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google
RCMOS - Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.2 2026 | Submission: 08/14/2026 | Accepted: 09/10/2026 | Publication: 10/24/2026

A method of compliance that corresponds to the size of the organization.

In this context, resilience is both a technical capability and a governance attribute.

ABNT NBR ISO 31000:2018 establishes that risk management must be integrated into all...

Organizational activities and that senior management is responsible for ensuring this integration (Brazilian Association of

Technical Standards, 2018). Recovery after an incident

It depends on previous decisions regarding backups, contracts with suppliers, and communication.

with clients and resource allocation, all situated within the realm of company management. The data from

IBM (2025) associated the reduction in the average cost of breaches with more accurate identification and containment.

quick responses confirm that preparing to respond is an investment with a return.

It is measurable and reinforces leadership's responsibility for its existence.

FINAL CONSIDERATIONS

This article examined the theoretical and normative foundations that underpin the attribution of security.

cybersecurity for senior management, with attention to small and medium-sized enterprises. The review demonstrated

that the topic has followed a path in the literature and technical references that starts from control

Technical aspects, moving through management and arriving at governance, reflect the growing dependence of organizations.

with regard to digital data and systems and the consequent increase in cyber risk to the status of

Strategic risk, with effects on the continuity, reputation and financial results of companies.

The evolution of the field has shown that information security is no longer understood as

ownership of systems and came to be seen as a result of the interaction between people, processes and

technology. The inclusion of the governing function in the NIST Cybersecurity Framework 2.0 and the requirements of

ISO/IEC 27001 leadership consolidates the understanding that the strategic direction of safety

It is up to the managers, with the technical teams responsible for implementing the controls defined from this.

direction.

Agency theory explained why the delegation of security, without information and communication mechanisms...

Control generates costs and exposes the organization to risks that the manager cannot foresee. The theory

from the upper echelons and the empirical studies that applied it indicated that the composition and the

Knowledge of senior management is associated with the occurrence of violations, which reinforces the

shared responsibility of the summit and dismisses the idea that the issue could be entrusted to a single person.

A single professional or an external supplier without supervision.

In legal terms, the duty of diligence stipulated in the Corporations Law and the Civil Code,

In addition to the security and governance obligations of the LGPD (Brazilian General Data Protection Law), it provides a regulatory basis to affirm...

that inaction in the face of cyber risk is incompatible with the standard of conduct required of

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google

Year VII, v.2 2026 | Submission: 08/14/2026 | Accepted: 09/10/2026 | Publication: 10/24/2026

administrators. The sanctions provided for in the legislation and the regulations of the national authority.
They give concrete form to this duty, bringing cybersecurity closer to other obligations of
Compliance measures that are already part of any administrator's routine.
The economics of security has shown that investment in protection should be decided based on...
The value of the information and the risk reduction achieved are managerial decisions. The data on the
cost of violations, even if derived from samples that do not specifically represent the
Small Brazilian businesses highlight the magnitude of the losses and show that the capacity of
Detection and containment directly influence the financial outcome, so preparedness is essential.
Responding to incidents should be understood as an investment, not an ancillary expense.
Analysis of the human factor revealed that most violations involve errors, manipulation, or
Organizational conditions that favor them. Awareness, consistency between discourse and practice.
and the correction of latent conditions created by management decisions appear as central elements.
from a culture of compliance capable of reducing the organization's exposure. This culture does not arise
spontaneously, as it depends on managerial decisions regarding training, internal communication and
Resource allocation.
The reliance on technology vendors has broadened the risk perimeter for companies and made them...
Cyber due diligence is an indispensable part of governance. The controller's responsibility for
Data processed by third parties, as stipulated in the LGPD (Brazilian General Data Protection Law), requires careful selection and contractual clauses.
adequate and proportionate supervision to the criticality of each relationship. In smaller companies, in
Which technological services are most commonly contracted? This due diligence represents a portion...
expressive of the security management itself.
As a contribution, the study proposes that small and medium-sized enterprises address cybersecurity.
as a business risk, under the direct responsibility of its managers, supported by measures
proportional to the size of the company, such as defining responsibilities, classifying suppliers, and providing training.
Backups and incident response plan. Further research is recommended.
empirically investigate the level of involvement of executives in smaller Brazilian companies.
Portability relates to the topic and its effects on the occurrence and cost of incidents.

REFERENCES

ANDERSON, R. Why information security is hard: an economic perspective. In: ANNUAL COMPUTER SECURITY APPLICATIONS CONFERENCE, 17., 2001, New Orleans. **Proceedings** [...]. Los Alamitos: IEEE Computer Society, 2001. p. 358-365.

ANDERSON, R.; MOORE, T. The economics of information security. **Science,** vol. 314, no. 5799, p. 610-613, 2006.

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google

Year VII, v.2 2026 | Submission: 08/14/2026 | Accepted: 09/10/2026 | Publication: 10/24/2026

Brazilian Association of Technical Standards. **ABNT NBR ISO 31000:** Risk management: guidelines. Rio de Janeiro: ABNT, 2018.

Brazilian Association of Technical Standards. **ABNT NBR ISO/IEC 27001:** Information security, cybersecurity and privacy protection: Information security management systems: requirements. Rio de Janeiro: ABNT, 2022a.

Brazilian Association of Technical Standards. **ABNT NBR ISO/IEC 27002:** Information security, cybersecurity and privacy protection: Information security controls.
Rio de Janeiro: ABNT, 2022b.

NATIONAL DATA PROTECTION AUTHORITY. **Guidance guide:** information security for small data processing agents. Brasília, DF: ANPD, 2021.

NATIONAL DATA PROTECTION AUTHORITY. Resolution CD/ANPD No. 2, of January 27, 2022. Approves the Regulation for the application of Law No. 13.709, of August 14, 2018, General Law on the Protection of Personal Data (LGPD), for small-scale data processing agents. **Official Gazette of the Union,** Brasília, DF, January 28, 2022.

NATIONAL DATA PROTECTION AUTHORITY. Resolution CD/ANPD No. 4, of February 24, 2023. Approves the Regulation on Dosimetry and Application of Administrative Sanctions.
Official Gazette of the Union, Brasília, DF, February 27, 2023.

NATIONAL DATA PROTECTION AUTHORITY. Resolution CD/ANPD No. 15, of April 24, 2024. Approves the Security Incident Reporting Regulation. **Official Gazette of the Union,** Brasília, DF, April 26, 2024.

BOYENS, J. et al. **Cybersecurity supply chain risk management practices for systems and organizations.** Gaithersburg: National Institute of Standards and Technology, 2022. (NIST Special Publication 800-161 Rev. 1).

BRAZIL. Law No. 6,404, of December 15, 1976. Provides for Corporations. **Official Gazette of the Union,** Brasília, DF, December 17, 1976.

BRAZIL. Law No. 10,406, of January 10, 2002. Establishes the Civil Code. **Official Gazette of the Union,** Brasília, DF, January 11, 2002.

BRAZIL. Law No. 13.709, of August 14, 2018. General Law on the Protection of Personal Data (LGPD).
Official Gazette of the Union, Brasília, DF, August 15, 2018.

BRAZIL. Decree No. 11,856, of December 26, 2023. Establishes the National Cybersecurity Policy and the National Cybersecurity Committee. **Official Gazette of the Union,** Brasília, DF, December 27, 2023.

BULGURCU, B.; CAVUSOGLU, H.; BENBASAT, I. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. **MIS Quarterly,** vol. 34, no. 3, p. 523-548, 2010.

CAVUSOGLU, H.; MISHRA, B.; RAGHUNATHAN, S. The effect of internet security breach

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google

Year VII, v.2 2026 | Submission: 08/14/2026 | Accepted: 09/10/2026 | Publication: 10/24/2026

announcements on market value: capital market reactions for breached firms and internet security developers. **International Journal of Electronic Commerce,** vol. 9, no. 1, p. 69-104, 2004.

D'ARCY, J.; HOVAV, A.; GALLETTA, D. User awareness of security countermeasures and their impact on information systems misuse: a deterrence approach. **Information Systems Research,** vol. 20, no. 1, p. 79-98, 2009.

DHILLON, G.; BACKHOUSE, J. Current directions in IS security research perspectives: towards socio-organizational. **Information Systems Journal,** vol. 11, no. 2, p. 127-153, 2001.

EISENHARDT, KM Agency theory: an assessment and review. **Academy of Management Review,** vol. 14, no. 1, p. 57-74, 1989.

FREUND, J.; JONES, J. **Measuring and managing information risk:** a FAIR approach. Oxford: Butterworth-Heinemann, 2015.

GIL, AC **How to prepare research projects.** 6th ed. São Paulo: Atlas, 2017.

GORDON, LA; LOEB, MP The economics of information security investment. **ACM Transactions on Information and System Security,** v. 5, no. 4, p. 438-457, 2002.

HAISLIP, J.; LIM, J.-H.; PINSKER, R. The impact of executives' IT expertise on reported data security breaches. **Information Systems Research,** vol. 32, no. 2, p. 318-334, 2021.

HAMBRICK, D.C.; MASON, PA Upper echelons: the organization as a reflection of its top managers. **Academy of Management Review,** vol. 9, no. 2, p. 193-206, 1984.

HERATH, T.; RAO, HR Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness. **Decision Support Systems,** vol. 47, no. 2, p. 154-165, 2009.

HUBBARD, DW; SEIERSEN, R. **How to measure anything in cybersecurity risk.** Hoboken: Wiley, 2016.

IBM. **Cost of a data breach report 2019.** Armonk: IBM Security, 2019.

IBM. **Cost of a data breach report 2020.** Armonk: IBM Security, 2020.

IBM. **Cost of a data breach report 2021.** Armonk: IBM Security, 2021.

IBM. **Cost of a data breach report 2022.** Armonk: IBM Security, 2022.

IBM. **Cost of a data breach report 2023.** Armonk: IBM Security, 2023.

IBM. **Cost of a data breach report 2024.** Armonk: IBM Security, 2024.

IBM. **Cost of a data breach report 2025:** the AI oversight gap. Armonk: IBM Security, 2025.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION. **ISO/IEC 27014:** information security, cybersecurity and

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google

Year VII, v.2 2026 | Submission: 08/14/2026 | Accepted: 09/10/2026 | Publication: 10/24/2026

privacy protection: governance of information security. Geneva: ISO, 2020.

JENSEN, MC; MECKLING, WH Theory of the firm: managerial behavior, agency costs and ownership structure. **Journal of Financial Economics,** vol. 3, no. 4, p. 305-360, 1976.

KWON, J. et al. The association between top management involvement and compensation and information security breaches. **Journal of Information Systems,** vol. 27, no. 1, p. 219-236, 2013.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **The NIST Cybersecurity Framework (CSF) 2.0.** Gaithersburg: NIST, 2024. (NIST Cybersecurity White Paper 29).

NELSON, A. et al. **Incident response recommendations and considerations for cybersecurity risk management:** a CSF 2.0 community profile. Gaithersburg: National Institute of Standards and Technology, 2025. (NIST Special Publication 800-61 Rev. 3).

POSTHUMUS, S.; VON SOLMS, R. A framework for the governance of information security. **Computers & Security,** vol. 23, no. 8, p. 638-646, 2004.

REASON, J. **Managing the risks of organizational accidents.** Aldershot: Ashgate, 1997.

SCHNEIER, B. **Secrets and lies:** digital security in a networked world. New York: John Wiley & Sons, 2000.

SIPONEN, M.; VANCE, A. Neutralization: new insights into the problem of employee information systems security policy violations. **MIS Quarterly,** vol. 34, no. 3, p. 487-502, 2010.

SNYDER, H. Literature review as a research methodology: an overview and guidelines. **Journal of Business Research,** vol. 104, p. 333-339, 2019.

SOOMRO, ZA; SHAH, MH; AHMED, J. Information security management needs more holistic approach: a literature review. **International Journal of Information Management,** vol. 36, no. 2, p. 215-225, 2016.

TORRACO, RJ Writing integrative literature reviews: guidelines and examples. **Human Resource Development Review,** vol. 4, no. 3, p. 356-367, 2005.

EUROPEAN UNION. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures to ensure a high common level of cybersecurity in the Union (SRI 2 Directive). **Official Journal of the European Union,** Luxembourg, L 333, p. 80-152, 27 Dec. 2022.

VERIZON. **2024 data breach investigations report.** Basking Ridge: Verizon Business, 2024.

VON SOLMS, B.; VON SOLMS, R. The 10 deadly sins of information security management. **Computers & Security,** vol. 23, no. 5, p. 371-376, 2004.

VON SOLMS, R.; VAN NIEKERK, J. From information security to cyber security. **Computers & Security,** vol. 38, p. 97-102, 2013.

WEICK, K.E.; SUTCLIFFE, KM **Managing the unexpected:** resilient performance in an age of

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google

Year VII, v.2 2026 | Submission: 08/14/2026 | Accepted: 09/10/2026 | Publication: 10/24/2026

uncertainty. 2nd ed. San Francisco: Jossey-Bass, 2007.

WILLIAMSON, OE **The economic institutions of capitalism:** firms, markets, relational contracting. New York: Free Press, 1985.

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.