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

Year VII, v.2 2026 | Submission: 06/05/2026 | Accepted: 09/06/2026 | Publication: 11/07/2026

The first hours after a cyberattack: detection, containment, evidence preservation, and recovery as determinants of organizational resilience.

The first hours after a cyberattack: detection, containment, evidence preservation and recovery as determinants of organizational resilience

The first few hours after a cyber attack: detection, containment, preservation of evidence and recovery as determinants of organizational resilience

Cassiano Rodolfo Jung
Master's student in Cybersecurity at American Global Tech University (AGTU). Specialist in Open Source Intelligence and Investigation (OSINT) from WB Educação. Specialist in Computer Forensics and Information Security from the Institute of Postgraduate and Undergraduate Studies (IPOG). Specialist in Strategic Management of Information Technology from Estácio de Sá University. Technologist in Information Security from the University of Vale do Rio dos Sinos (UNISINOS).

SUMMARY

The interval between the discovery of a cyber incident and the first response decisions involves choices that are difficult to reverse, such as isolating or keeping systems operational, preserving or discarding volatile traces, and communicating or waiting for confirmation of the facts. This article analyzes how detection, containment, preservation of digital evidence, regulatory communication, and operational recovery, when conducted in the first few hours, condition an organization's ability to resume its activities after an attack. This is a qualitative, exploratory, and descriptive study, constructed through a narrative review of the scientific literature and documentary analysis of technical standards, government guidelines, sectoral reports, and legislation. The results indicate that the intruder's dwell time in the environment, the order of collection of volatile data, the availability of isolated backups, and the prior existence of defined roles and decision-making channels explain a large part of the difference between contained incidents and prolonged crises. It can be concluded that the quality of the initial response depends less on technical improvisation and more on organizational preparedness, which requires treating incident response as a risk management capability, linked to governance, digital expertise, and business continuity.

Keywords: Incident response. Computer forensics. Ransomware. Business continuity. Cyber resilience.

ABSTRACT

The interval between the discovery of a cyber incident and the first response decisions concentrates choices that are hard to reverse, such as isolating or keeping systems online, preserving or discarding volatile traces, and notifying stakeholders or waiting for facts to be confirmed. This article examines how detection, containment, digital evidence preservation, regulatory operational communication and recovery, when carried out in the first hours, shape an organization's ability to resume operations after an attack. It is a qualitative, exploratory and descriptive study based on a narrative review of the scientific literature and on documentary analysis of technical standards, government guidance, industry reports and legislation. The findings indicate that attacker dwell time, the order in which volatile data are collected, the availability of isolated backups and the prior definition of decision roles and channels account for much of the difference between contained incidents and prolonged crises. The study concludes that the quality of the initial response depends less on technical improvisation than on organizational preparedness, which requires treating incident response as a risk management capability linked to governance, digital forensics and business continuity.
Keywords: Incident response. Digital forensics. Ransomware. Business continuity. Cyber resilience.

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: 06/05/2026 | Accepted: 09/06/2026 | Publication: 11/07/2026

1 INTRODUCTION

Information security incidents are no longer rare events, dealt with in isolation by
Technology teams have become integrated into the risk management routine of organizations of all sizes.
A report on data breach investigations published by Verizon in 2025 analyzed more than
22,000 incidents, of which 12,195 were confirmed as violations, and recorded the presence of
Ransomware was involved in 44% of these cases (Verizon, 2025). During the same period, the study conducted by
The Ponemon Institute for IBM estimated the average global cost of a breach at US$4.44 million.
and the average identification and containment cycle is 241 days (IBM, 2025). These numbers reveal that
frequency of the problem and also the duration of its effects, which extend far beyond the
The moment when the attack is noticed.

Between the discovery of an attack and the stabilization of the environment, there is a short window in which decisions...
Decisions of great consequence need to be made with incomplete information. Shutting down a server.
It can stop the spread of malicious code and, at the same time, erase it from memory.
volatile traces that would allow reconstruction of the intrusion. Quickly restoring the systems can
to reduce operational losses, but also to reintroduce the intruder if the original access route fails.
once it has been identified. Communicating too early can lead to inaccurate information, while
Communicating too late can violate legal deadlines and compromise the trust of clients and regulators. This work
focuses on this set of tensions.

The aim of this article is to analyze how the detection, containment, and preservation of digital evidence,
regulatory communication and operational recovery, when conducted in the first few hours after
The discovery of an incident influences an organization's ability to recover. Part-
If the hypothesis is that the quality of this initial response results more from prior preparation, it is expressed
in defined roles, tested procedures, and isolated recovery infrastructure, rather than
Technical skills mobilized during a crisis. To support this discussion, the text articulates
international technical standards, academic studies on response teams, sector reports
with recent empirical data and applicable Brazilian legislation, as well as documented cases
publicly.

2 METHODOLOGY

The research adopts a qualitative approach, of an exploratory and descriptive nature, as proposed.
by Gil (2008), for whom exploratory studies seek to provide greater familiarity with
A problem is identified, while descriptive variables seek to characterize phenomena and establish relationships between variables.

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: 06/05/2026 | Accepted: 09/06/2026 | Publication: 11/07/2026

The choice is justified by the multidisciplinary nature of the topic, which involves technical aspects, organizational, legal and management factors, and the lack of a single database capable of measuring, Similarly, the effect of decisions made in the first hours of an incident. For this reason... Therefore, the study prioritizes the integration of diverse sources rather than statistical measurement. from a single dataset.

Regarding the procedures, bibliographic research and documentary research were combined. The literature review followed the narrative review format, which, according to Rother (2007), is appropriate to describe and discuss the state of the art of a subject from a theoretical and contextual point of view, without The intention to exhaust all sources or to apply systematic search and selection criteria. They were consulted articles published in peer-reviewed journals, such as *Computers & Security, Information & Management, International Journal of Information Management, Human Factors* and *Frontiers in Psychology,* identified through searches on Google Scholar and on the portals of their respective publishers, in addition to reference works in digital forensics and organizational management. High reliability.

The document analysis included technical publications from the National Institute of Standards and Technology (NIST), standards from the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), Internet Engineering document RFC 3227 Task Force, the joint U.S. agency guide on *ransomware,* the General Data Protection Act. Personal Data Protection Law, the Code of Criminal Procedure with the amendments introduced by Law No. Law 13.964/2019 and Resolution CD/ANPD No. 15/2024 were examined. Sectoral reports were also reviewed. with empirical data widely cited in the literature, published by Mandiant, IBM, Verizon and Sophos, and public records of two high-profile incidents, the NotPetya attack on The AP Møller-Maersk company in 2017, and the *ransomware* attack on Colonial Pipeline in 2021.

The material was organized into six thematic areas, defined based on the response phases described. in the reference standards, namely, response models, detection, containment, preservation of evidence, communication, and recovery. In each area, the aim was to compare what the standards They recommend what empirical studies and documented cases reveal about the practice.

It is acknowledged as a limitation that the sector reports are produced by companies. Private, with their own samples and methodologies that do not allow for direct comparison between them. By That is, their numbers are treated as trend indicators, not as exact measures of... phenomenon.

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: 06/05/2026 | Accepted: 09/06/2026 | Publication: 11/07/2026

3 REFERENCE MODELS FOR INCIDENT RESPONSE AND THEIR EVOLUTION

For more than a decade, the main international reference for organizing the response to
The incidents were the second revision of NIST Special Publication 800-61, prepared by Cichonski *et al.*
al. (2012). The document describes a cycle composed of four phases: preparation, detection, and
analysis, containment, eradication and recovery, and post-incident activities, and emphasizes that the response
It doesn't end with the restoration of the systems, as the lessons learned must return to the phase of
preparation. The guide also recommends that organizations formalize policies, plans and
response procedures and define the structure and roles of the responsible team, which allows that
The process should be documented, communicated to managers, and verified through internal and external audits.
In the field of international standardization, the ISO/IEC 27035 series plays a similar role. The edition
The first part of the 2023 standard organizes incident management into five phases: planning.
and preparation, detection and notification, assessment and decision, responses and lessons learned (ISO,
2023). The separation between detection and the assessment and decision phase is especially relevant for the
The topic of this article is that it recognizes that not every detected event constitutes an incident and that...
Correct classification, done right at the beginning, determines the scale of resources mobilized. Cichonski *et*
al. (2012) observe, in this sense, that for many organizations the most difficult part of the process is
precisely to detect and accurately assess potential incidents, distinguishing precursors,
Indicators and false positives amid a large volume of alerts.
In April 2025, NIST published the third revision of SP 800-61, authored by Nelson *et al.* (2025).
which replaces the 2012 version and significantly alters the perspective adopted. Instead of a
In its own cycle, incident response is now described as a community-based cybersecurity profile.
Framework 2.0, distributed among the six functions of the model: govern, identify, protect, detect,
Respond and recover (NIST, 2024). According to the authors, incident response should be incorporated
to cybersecurity risk management activities, so that preparation, reducing the number
and the impact of incidents and the improvement of detection, response and recovery should be addressed in
integrated form (Nelson *et al.,* 2025). From this perspective, the response ceases to be an activity
triggered only when something goes wrong and becomes dependent on governance and inventory decisions.
of assets and preventive controls taken before the attack.
Academic literature confirms that the gap between the normative model and practice is real. Tøndel,
Line and Jaatun (2014) conducted a systematic review on security incident management and
They organized the reported practices according to the phases of ISO/IEC 27035, concluding that the practice
The observed behavior is, broadly speaking, consistent with the standard, but identifying which recommendations are...
They are more difficult to follow in the daily operations of organizations. Baskerville, Spagnoletti and Kim

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: 06/05/2026 | Accepted: 09/06/2026 | Publication: 11/07/2026

(2014), based on a comparative case study in three European organizations, showed that the Security strategies tend to prioritize the prevention of predictable threats, although... Responsiveness is essential for dealing with unpredictable threats, which requires a deliberate balance between the two paradigms.

Another recurring point in the literature is the disconnect between response teams and strategic management. of security. In a case study on incident response in practice, Ahmad, Hadgkiss and Ruighaver (2012) observed that the organization analyzed closely followed industry best practices. but focused its efforts on technical aspects and business continuity, neglecting to carry out Learning activities following incidents. In a subsequent study, conducted in an organization Australian financial institution, Ahmad, Maynard and Shanks (2015) identified systemic deficiencies in poor response practices and lack of communication between those responsible for incidents and management. security, which prevents the organization from learning from its own attacks. Table 1 summarizes the correspondence between the three models discussed in this section, showing that, despite the Despite differences in terminology, all reserve specific steps for preparation, detection, and... Learning after the incident.

Table 1 – Correspondence between reference models for incident response

NIST SP 800-61 Rev. 2 (2012)	ISO/IEC 27035-1 (2023)	NIST SP 800-61 Rev. 3 and CSF 2.0 (2025)
Preparation	Planning and preparation	Govern, Identify and Protect
Detection and analysis	Detection and notification, Evaluation and decision	Detect
Containment, eradication and recovery	Answers	Respond and Retrieve
Post-incident activities	Lessons learned: Identify (continuous improvement)	

Source: prepared by the author based on Cichonski et al. (2012), ISO (2023), NIST (2024) and Nelson et al. (2025).

4. Intruder Detection and Residency Time

The expression "first hours" presupposes that the incident was noticed, but in practice, the response Conditioning begins much earlier, by the interval during which the invader remains in the environment without to be noticed. Mandiant, the incident response division of Google Cloud, measures this interval by This indicator is known as *"dwell time,"* defined as the number of days between the start of the intrusion and Your identification. According to the M-Trends 2025 report, the global median for this time was 11 days.

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.

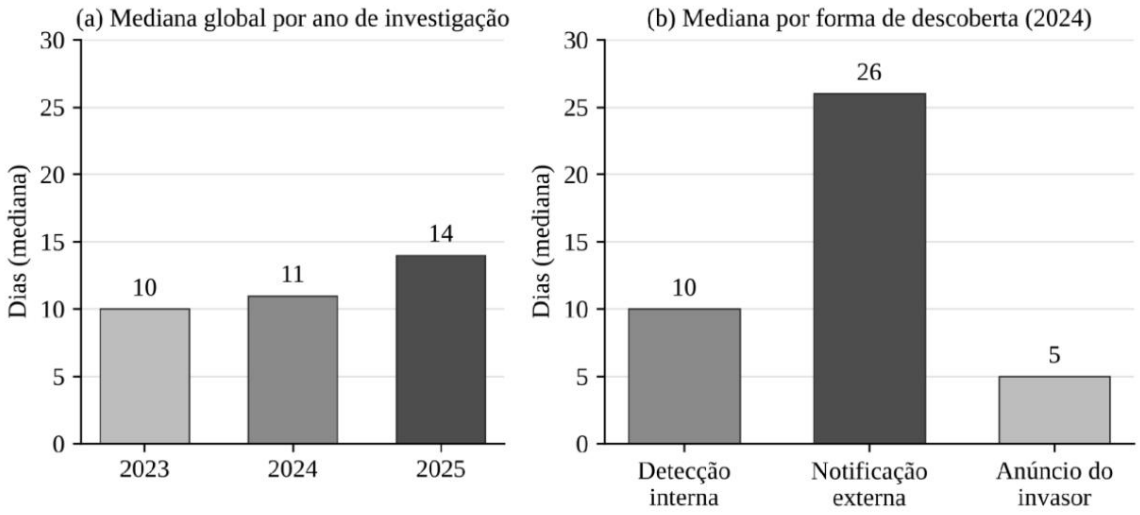
Machine Translated by Google
RCMOS - Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.2 2026 | Submission: 06/05/2026 | Accepted: 09/06/2026 | Publication: 11/07/2026

in investigations conducted in 2024, slightly above the 10 days observed in 2023
(Mandiant, 2025). The following edition recorded a further increase, with a median of 14 days in
investigations from 2025 (Mandiant, 2026).

More revealing than the global median is the contrast between the methods of discovery. In investigations
From 2024, when the organization itself identified the malicious activity, the median was 10 days.
while in cases where the discovery came from an external entity, it took up to 26 days. When
The attacker himself announced his presence, a typical situation in *ransomware* attacks where the note
The first sign perceived is that of rescue, the median dropped to 5 days (Mandiant, 2025). Figure 1
presents these values. The value of 5 days should not be interpreted as a sign of defensive efficiency, because,
In these cases, the discovery does not result from monitoring the victim, but rather from the attacker's decision to...
If it is revealed, this puts the organization in a position to respond under maximum pressure.

Figure 1 – Median time the invader remains in the environment, in days



Source: compiled by the author with data from Mandiant (2025; 2026).

The numbers from Mandiant and those from IBM measure distinct phenomena and should not be confused.
While Mandiant calculates the median dwell time in the intrusions it investigated, the
An IBM study estimates the average number of days needed to identify and contain a data breach.
including the restoration of services, in a sample of 600 organizations. Still, both
They point in the same direction. The cycle measured by IBM fell to 241 days in the 2025 study, the shortest.
The level is nine years and 17 days below the previous year's result, suggesting efficiency gains.
which, although relevant, still leave organizations exposed for months (IBM, 2025).

The ability to detect early depends on visibility and method. The chain model of
The intrusion proposed by Hutchins, Cloppert, and Amin (2011) describes the attack as a sequence 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
IRCMOS – Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.2 2026 | Submission: 06/05/2026 | Accepted: 09/06/2026 | Publication: 11/07/2026

The process, from recognizing and executing objectives, is outlined, and it argues that the defender can frustrate the...
An adversary operation can be disrupted by interrupting any of them. The MITRE ATT&CK knowledge base,
described by Strom *et al.* (2018), further developed this logic by cataloging tactics and techniques effectively.
observed in real attacks, allowing monitoring teams to formulate hypotheses of
Behavior-driven detection, not just detection based on known code signatures.
More recent data shows why this matters, as the exploitation of vulnerabilities has responded
Voice phishing accounted for 32% of intrusions investigated in 2025, and voice *phishing* reached 11% (Mandiant, 2026).
Detection is not just a problem of tools, but also of cognition. Endsley (1995)
He described situational awareness on three levels: perception of environmental elements,
understanding its meaning and projecting its future state, and showed that failures in any
One of them compromises decision-making in dynamic systems. By analogy, applied to a
Security operations center, the model can help explain why an alert correctly
The generated event can be ignored when the analyst perceives the event but does not understand its relationship to it.
other signs, or because an intrusion understood too late no longer allows for effective containment.
Van der Kleij, Kleinhuis and Young (2017), while investigating response teams in the Netherlands,
They proposed a needs model that distributes performance factors across levels.
organizational, team, individual, and instrumental, indicating that performance problems may
originating at any of these levels or in a combination thereof.

5. Containment and Decision-Making Under Pressure

Containment is the phase in which incident response produces its most immediate effects on the
Organization operation. Cichonski *et al.* (2012) recommend that the containment strategy be
chosen based on predefined criteria, including the potential for harm and
resource subtraction, the need to preserve evidence, the availability of services, the
The time and resources required, the expected effectiveness of the measure, and the duration of the solution. The authors
They also recommend that organizations develop distinct containment strategies for each type.
main incident report, with clearly documented criteria, precisely to facilitate decision-making.
decision when the incident occurs.
The Colonial Pipeline case illustrates the scale that these decisions can reach. According to the testimony
from the company's then-president to the Committee on Homeland Security and Governmental Affairs of
In the U.S. Senate, an employee found a ransom note in a network system.
Information technology shortly before 5:00 AM on May 7, 2021, and at 6:10 AM the company
confirmed that the approximately 5,500 miles of pipelines, equivalent to roughly 8,850

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: 06/05/2026 | Accepted: 09/06/2026 | Publication: 11/07/2026

kilometers had been paralyzed (Blount, 2021). The network transported almost half of
fuel consumed on the east coast of the United States, and the operation only began to resume.
on the night of May 12th. The same testimony attributes the initial access to a legacy network profile.
A virtual private network (VPN) that should not be in use.
The episode shows that containment may require the deliberate interruption of operations before...
Find out if they were affected. In the same testimony, the executive stated that the shutdown sought to isolate
and contain the attack to prevent the malicious code from spreading to the technology network.
operational, which controls the pipelines, in case this had not already occurred, and acknowledged that the company
At that moment, I did not know either the point of origin or the extent of the attack (Blount, 2021).
The interval of just over an hour between the discovery and the total shutdown indicates that a decision
This measure of this magnitude was taken before any complete diagnosis, which reinforces the recommendation.
Cichonski *et al.* (2012) recommend documenting containment criteria beforehand.
The joint guide on *ransomware* published by the US cybersecurity agency and
Infrastructure, in partnership with other agencies, recommends determining which systems were affected.
and isolate them immediately, disconnecting the network at the switch level when the
commitment for broad (CISA, 2023). The same document advises that the equipment only
They should be switched off when it is not possible to disconnect them from the network, warning that the shutdown...
eliminates evidence stored in volatile memory. The guide also recommends the use of channels for
Alternative communication methods, such as phone calls, are used to prevent the intruder from eventually...
present in mail and messaging systems, monitor the coordination of the response and anticipate the
containment measures.
The literature on high-reliability organizations offers a useful lens for understanding this.
behavior. Weick and Sutcliffe (2015) identify five principles that distinguish organizations
capable of operating in high-risk environments with a low incidence of serious failures, the concern
with failure, the reluctance to simplify interpretations, the sensitivity to operations, the
commitment to resilience and deference to technical competence. This last principle is
particularly relevant to containment, as it proposes that, in critical situations, the decision-making authority
Switch to whoever has the most accurate knowledge about the problem, regardless of...
hierarchical position. Applied to a cyber incident, the principle suggests that the analyst who
understands the mechanics of the attack and has direct access to who can authorize the interruption of
systems.

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: 06/05/2026 | Accepted: 09/06/2026 | Publication: 11/07/2026

6. PRESERVATION OF DIGITAL EVIDENCE IN THE FIRST HOURS

The pressure to resume operations tends to put the preservation of evidence second.
plan, although the technical guidelines are clear regarding the priority of data collection over interventions.
Corrective measures. The RFC 3227 document, prepared by Brezinski and Killalea (2002), establishes that the collection
It should follow the order of volatility, starting with the registers and cache memory, then moving on.
through routing tables, the process table, and main memory, through the systems of
temporary files and disk access, all the way to remote records, network topology, and media.
archiving. The same document recommends not shutting down the system before completing the collection.
and not trust the programs installed on the compromised machine, which may have been altered by
invader.

Kent *et al.* (2006), in the NIST guide dedicated to integrating forensic techniques into incident response,
They describe the forensic process in four stages: collection, examination, analysis, and reporting, and they call it...
Please note that many decisions made during the response, such as restarting a server, are subject to change.
Applying a correction, or doing so, irreversibly alters the state of the data. For this reason, the authors
They recommend that organizations have forensic capabilities, supported by policies and
Procedures that guide, among other activities, the collection of volatile data before shutdown.
of the systems. Similar guidance appears in the guide on *ransomware,* which recommends capturing
image and memory of a sample of the affected equipment (CISA, 2023).

In the international regulatory framework, ISO/IEC 27037 establishes guidelines for the identification,
collection, acquisition and preservation of digital evidence (ISO, 2012). The standard states that the
The treatment of this evidence must be auditable, repeatable, reproducible, and justifiable, so that
a third party can evaluate the actions taken and, where applicable, obtain the same results from
from the same data. Casey (2011) adds that the integrity of digital evidence depends on
Rigorous documentation of each action performed, using *hash* functions to demonstrate that the
The data were not altered, and this reflects an understanding of the limitations of the tools employed, given that...
Digital evidence is, by its nature, easy to modify without leaving obvious traces.

In Brazil, the preservation of evidence gained more precise legal contours with Law No.
Law 13.964/2019, which inserted articles 158-A to 158-F into the Code of Criminal Procedure and defined the chain of
custody as the set of procedures used to maintain and document history
chronological record of the trace, from its recognition to its disposal (Brazil, 2019). Article 158-B
It details the stages of this process, which include recognition, isolation, fixation, collection, and...
Packaging, transportation, receiving, processing, storage, and disposal.

The legal text does not distinguish the nature of the trace, so its requirements also apply 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: 06/05/2026 | Accepted: 09/06/2026 | Publication: 11/07/2026

Digital traces and mistakes made in the first few hours can compromise the use of...
evidence in any eventual criminal prosecution arising from the incident.
The tension between preserving and restoring, therefore, is not resolved by choosing one of the extremes. The guide
Regarding *ransomware,* it proposes an intermediate solution by recommending image capture and...
memory of a sample of the affected equipment, and not all of it, which allows for gathering elements.
for investigation without paralyzing recovery (CISA, 2023). The application of this strategy, however,
This presupposes procedures for the secure collection and storage of images that are defined beforehand.
incident, as recommended by Kent *et al.* (2006). Without this preparation, immediate restoration tends
to erase the traces that would allow identification of the entry route, the extent of the compromise and the
potential data loss, with the consequent risk of reinfection, which the guide itself warns about.
when discussing the recovery phase.

7. Communication, Governance and Regulatory Obligations

Communication during an incident involves distinct audiences, each with their own needs and deadlines.
own, such as senior management, internal teams, customers, suppliers, authorities
regulatory bodies and, in some cases, security forces and the press. The introduction of the governing function.
The Cybersecurity Framework 2.0 recognizes that defining roles, responsibilities, and
Cybersecurity authority is the responsibility of the organization's management, not just the technical department.
(NIST, 2024). In incident response, this definition translates to knowing, before the crisis, who decides.
Regarding external communication, who speaks on behalf of the company and what information can be shared?
disclosed without jeopardizing the investigation or containment efforts.
In the Brazilian legal system, article 48 of the General Law on the Protection of Personal Data determines 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 harm to data subjects (Brazil, 2018).
The deadline was set by Resolution CD/ANPD No. 15, of April 24, 2024, which establishes three days.
Useful, counted from the knowledge that the incident affected personal data, both for communication purposes.
to the authority regarding communication to the holders, allowing for substantiated supplementation based on
up to twenty working days and double the time for small data processing agents (ANPD, 2024). A
The same rule requires that the incident record be kept for at least five years, inclusive.
when there is no communication.
The resolution also defines objective criteria for characterizing relevant risk or harm, requiring
that the incident may significantly affect the fundamental interests and rights of the holders and that
involve at least one specific type of data, such as sensitive data, data of children, adolescents

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: 06/05/2026 | Accepted: 09/06/2026 | Publication: 11/07/2026

or elderly people, financial data, authentication data, data protected by confidentiality, or large-scale data.
scale (ANPD, 2024). As the communication deadline is counted in working days from the
Given the nature of the incident, this classification needs to begin in the first few hours, when the
The extent of the commitment is still uncertain. The integration between the technical team, responsible for
to determine what data was accessed, and who is responsible for processing personal data.
The law mandates dialogue with the authority and the relevant parties, thus making it a requirement.
operational, and not just a recommendation for good governance.
Other jurisdictions adopt similarly short deadlines, which directly affects organizations with
international operations. The General Data Protection Regulation of the European Union, in
Article 33 stipulates that any breach of personal data must be reported to the supervisory authority.
without undue delay and, whenever possible, within 72 hours of the person responsible having had
knowledge of the fact (European Union, 2016). In the United States, the rule approved by the Securities
The Exchange Commission in 2023 will require publicly traded companies to disclose incidents.
cybersecurity measures deemed material within four business days of the determination of
materiality (United States, 2023). The overlap of these deadlines requires organizations to maintain
Communication templates and approval workflows are ready before any incident.
Communication with suppliers and partners has gained importance as the attacks have progressed.
to explore trust relationships between companies. Verizon's 2025 report indicates that...
Third-party involvement in violations has doubled, reaching 30% of the cases analyzed (Verizon, 2025).
This means that, in a considerable number of incidents, the response requires coordination with
External organizations, whose processes, timelines, and priorities may differ from those of the victim.
The experience reported by Ahmad, Maynard, and Shanks (2015) further shows that the lack of communication
Internal conflicts between response and security management hinder organizational learning, suggesting
that communication should be treated as part of the response process itself, with records that
feed into the subsequent review of the incident.

8. RECOVERY, BUSINESS CONTINUITY AND THE ROLE OF COPIES SECURITY

Recovery is often treated as the final stage of the response, but its conditions
Success factors are defined long before the incident. The NIST guide to contingency planning,
Developed by Swanson *et al.* (2010), it is recommended that the organization conduct an impact analysis.
In business, the goal is to establish, for each system, the maximum tolerable downtime.
recovery time objective and recovery point objective, which expresses the quantity

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: 06/05/2026 | Accepted: 09/06/2026 | Publication: 11/07/2026

The maximum amount of data that can be allowed to be lost. ISO 22301 incorporates these definitions into a management system.
of business continuity, with requirements for planning, operation, performance evaluation and
Continuous improvement (ISO, 2019). Without these parameters, the team lacks an objective criterion to define
the restoration order, which the guide itself links to the results of the impact analysis.

The role of backups has changed significantly with the professionalization of attacks.
ransomware . In a Sophos survey of 5,000 technology and security leaders in 14 countries,
94% of organizations hit by *ransomware* reported that attackers attempted to compromise the organization.
their backups during the attack, and 57% of these attempts were successful (Sophos, 2024a). The
The same study estimated the average cost of recovery, excluding any potential rescue payments, at
US$2.73 million. The most recent data from Mandiant (2026) confirms the trend, registering
ransomware groups are targeting their efforts towards backup infrastructure, in order to
Identity services and virtualization management platforms.

The case of AP Møller-Maersk, hit by NotPetya on June 27, 2017, became a benchmark.
on the fragility of recovery strategies. According to a report by Greenberg (2018), the
Malicious code destroyed the company's domain controllers worldwide, and reconstruction...
The infrastructure was only possible because a single controller, installed in an office in Ghana,
It was disconnected from the network due to a power outage at the time of the attack. The company
It rebuilt approximately 4,000 servers and 45,000 computers; the network was restored in ten days and the...
The chairman estimated the loss to be between US$250 million and US$300 million.
The episode shows that the recovery depended on chance, and not on an isolated copy kept from
planned form.

The technical lessons learned from these cases were incorporated into the official recommendations. The joint guide on
The ransomware instructs that data be restored from disconnected backups and
encrypted, following a priority order based on critical services, and alerts to the risk.
of reinfecting already cleaned systems during restoration (CISA, 2023). Ross *et al.* (2021), in the guide to
NIST, in its work on resilient systems engineering, proposes that cyber resilience be structured...
centered around four objectives—anticipate, resist, recover, and adapt—an approach that starts from
The assumption is that protection can fail, and the goal is to ensure the continuity of essential functions.
even in adverse conditions.

The decision regarding the payment of a ransom is also linked to the availability of the company's own means of...
recovery. In a survey of 2,974 professionals from organizations affected by *ransomware,*
Sophos verified that the victims whose backups were compromised paid the ransom.
in 67% of cases, compared to 36% among those who kept their copies intact, and that only 26% of
The first group recovered fully within a week, compared to 46% of the others (Sophos, 2024b).

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: 06/05/2026 | Accepted: 09/06/2026 | Publication: 11/07/2026

An IBM study recorded that the proportion of victims who refused to pay rose from 59% to 63%.
in 2025 (IBM, 2025). The recovery capacity, however, depends on tested plans. Grance *et*
al. (2006) argue that information technology plans should be subject to programs
Regular testing, training, and exercises, including table simulations and functional exercises.
precisely to reveal flaws that would only become apparent during a real crisis.

9 CONCLUSION

This article started from the premise that the first hours after the discovery of a cyberattack
They focus on decisions whose effects extend over weeks or months. The analysis of the literature, of
Technical standards, sectoral reports, and documented cases confirm this premise and allow
To qualify it. Initial decisions are indeed crucial, but their quality is rarely produced.
at the moment of the crisis, as it results from conditions created before the incident, such as the definition of roles,
the existence of tested procedures and the availability of isolated recovery infrastructure
from the production environment.
The evolution of reference models expresses this understanding. The replacement of the self-cycle
The second revision of SP 800-61, through a profile integrated with the Cybersecurity Framework 2.0, indicates that
Incident response is no longer conceived as a technical activity activated only in specific situations.
exceptional and came to be understood as risk management capability, linked to
governance. Academic literature reinforces this interpretation by demonstrating the persistent disconnect between
Response teams and strategic security management, which limits the ability of organizations to
Learn from your own incidents.
In terms of detection, the data shows that the intruder's dwell time continues to be measured in
days, and the global median rose from 10 to 14 days between the 2023 and 2025 surveys.
contrast between internal discovery, external notification, and the announcement made by the attacker himself.
This demonstrates that the way the incident is perceived determines the available room for maneuver.
When the first signal is the ransom note, the response starts at a disadvantage, because the opponent already...
It achieved its objectives. Investing in visibility, behavior-driven detection, and in
Therefore, team situational awareness means investing in the quality of the first few hours.
Regarding containment, the sources analyzed converge on the importance of decision criteria.
defined in advance, with clear authority to stop operations and channels of
Alternative communication methods allow for quick action without acting blindly. The case of Colonial.
Pipeline shows that preventive interruption of operations may be necessary even before...
Knowing the origin and scope of the attack is only feasible when the organization knows who has it.

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: 06/05/2026 | Accepted: 09/06/2026 | Publication: 11/07/2026

legitimacy to make this decision and what criteria support it. The principles of organizations of
High reliability provides a consistent theoretical foundation for this practice.
The preservation of digital evidence has proven to be a critical issue, exposed to the risk of being sacrificed.
In the name of speed. The order of volatility, the principles of auditability and reproducibility and
the chain of custody requirements stipulated in the Brazilian Code of Criminal Procedure converge towards
The same conclusion is reached that data collection needs to occur before corrective interventions. The loss of these
The evidence undermines the investigation, the accountability of the perpetrators, and the very security of the organization.
Recovery, as it prevents knowing if the intruder's access was effectively eliminated. Preparation
Forensic analysis should be treated as an integral part of the response, not as an ancillary activity.
Regulatory obligations add a temporal dimension that cannot be ignored. The deadline
three working days set by the National Data Protection Authority, added to the deadlines of other
In some jurisdictions, it is required that risk assessments for policyholders begin within the first few hours, with
Effective integration between the technical team and the person in charge of processing personal data.
The increasing involvement of third parties in violations amplifies this requirement, as communication becomes more...
Involve supply chains whose processes are not always aligned with those of the organization.
affected.

In the recovery section, the data on attacks targeting backups and the case of...
Maersk shows that the existence of a copy is not enough; it is necessary that it be isolated.
complete and restorable within the timeframe defined by the business impact analysis.
The data links compromised backups to a higher propensity to pay.
Rescue efforts and slower recovery indicate that the body's own recovery capacity expands the
The organization's margin of decision regarding extortion. This margin, however, only exists when the
Business continuity plans are exercised periodically and adjusted based on identified failures.
One limitation is that a significant portion of the empirical data used comes from reports.
sectoral studies developed by private companies, with different samples and methodologies, which prevents
Direct comparisons are not recommended, and caution is advised when generalizing the results. For further research, it is suggested...
Future plans include conducting empirical studies with Brazilian organizations to assess the relationship between
maturity in incident response, recovery time, and compliance with regulatory deadlines.
as well as investigations into the application of the chain of custody to digital traces in incidents
corporate. Such studies would allow us to verify, in a national context, the central hypothesis being supported.
in this work.

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: 06/05/2026 | Accepted: 09/06/2026 | Publication: 11/07/2026

REFERENCES

AHMAD, Atif; HADGKISS, Justin; RUIGHAVER, AB Incident response teams: challenges in supporting the organizational security function. **Computers & Security,** [Amsterdam], v. 31, no. 5, p. 643-652, 2012.

AHMAD, Atif; MAYNARD, Sean B.; SHANKS, Graeme. A case analysis of information systems and security incident responses. **International Journal of Information Management,** [Amsterdam], v. 35, no. 6, p. 717-723, 2015. DOI: 10.1016/j.ijinfomgt.2015.08.001.

NATIONAL DATA PROTECTION AUTHORITY (ANPD). **Resolution CD/ANPD No. 15, of April 24, 2024.** Approves the Security Incident Reporting Regulation. Brasília, DF: ANPD, 2024.

BASKERVILLE, Richard; SPAGNOLETTI, Paolo; KIM, Jongwoo. Incident-centered information security: managing a strategic balance between prevention and response. **Information & Management,** [Amsterdam], v. 51, no. 1, p. 138-151, 2014. DOI: 10.1016/j.im.2013.11.004.

BLOUNT, Joseph A. **Testimony of Joseph A. Blount, Jr., President and Chief Executive Officer, Colonial Pipeline Company, before the United States Senate Committee on Homeland Security and Governmental Affairs.** Washington, DC: US Senate, 8 June. 2021.

BRAZIL. **Law No. 13.709, of August 14, 2018.** General Law on the Protection of Personal Data (LGPD). Brasilia, DF: Presidency of the Republic, 2018.

BRAZIL. **Law No. 13,964, of December 24, 2019.** Improves criminal and criminal procedure legislation. Brasília, DF: Presidency of the Republic, 2019.

BREZINSKI, Dominique; KILLALEA, Tom. **Guidelines for evidence collection and archiving.** RFC 3227. [S. l.]: Internet Engineering Task Force, 2002.

CASEY, Eoghan. **Digital evidence and computer crime:** forensic science, computers and the internet. 3rd ed. Waltham: Academic Press, 2011.

CICHONSKI, Paul; MILLAR, Tom; GRANCE, Tim; SCARFONE, Karen. **Computer security incident handling guide.** Gaithersburg: National Institute of Standards and Technology, 2012. (NIST Special Publication 800-61, rev. 2). DOI: 10.6028/NIST.SP.800-61r2.

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA) *et al.* **#StopRansomware guide.** Washington, DC: CISA, 2023.

ENDSLEY, Mica R. Toward a theory of situation awareness in dynamic systems. **Human Factors,** [Thousand Oaks], vol. 37, no. 1, p. 32-64, 1995. DOI: 10.1518/001872095779049543.

GIL, Antonio Carlos. **Methods and techniques of social research.** 6th ed. São Paulo: Atlas, 2008.

GRANCE, Tim; NOLAN, Tamara; BURKE, Kristin; DUDLEY, Rich; WHITE, Gregory; GOOD, Travis. **Guide to testing, training, and exercise programs for IT plans and capabilities.** Gaithersburg: National Institute of Standards and Technology, 2006. (NIST Special Publication 800-84).

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: 06/05/2026 | Accepted: 09/06/2026 | Publication: 11/07/2026

GREENBERG, Andy. The untold story of NotPetya, the most devastating cyberattack in history. **Wired,** San Francisco, 22 Aug. 2018.

HUTCHINS, Eric M.; CLOPPERT, Michael J.; AMIN, Rohan M. **Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains.** Bethesda: Lockheed Martin Corporation, 2011.

IBM. **Cost of a data breach report 2025.** Armonk: IBM Corporation, 2025.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). **ISO/IEC 27037:** information technology, security techniques, guidelines for identification, collection, acquisition and preservation of digital evidence. Geneva: ISO, 2012.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). **ISO 22301:** security and resilience, business continuity management systems, requirements. Geneva: ISO, 2019.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). **ISO/IEC 27035-1:** information technology, information security incident management, part 1, principles and process. Geneva: ISO, 2023.

KENT, Karen; CHEVALIER, Suzanne; GRANCE, Tim; DANG, Hung. **Guide to integrating forensic techniques into incident response.** Gaithersburg: National Institute of Standards and Technology, 2006. (NIST Special Publication 800-86).

MANDIANT. **M-Trends 2025.** Mountain View: Google Cloud, 2025.

MANDIANT. **M-Trends 2026.** Mountain View: Google Cloud, 2026.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). **The NIST Cybersecurity Framework (CSF) 2.0.** Gaithersburg: NIST, 2024. (NIST Cybersecurity White Paper 29). DOI: 10.6028/NIST.CSWP.29.

NELSON, Alexander; REKHI, Sanjay; SOUPPAYA, Murugiah; SCARFONE, Karen. **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). DOI: 10.6028/NIST.SP.800-61r3.

ROSS, Ron; PILLITTERI, Victoria; GRAUBART, Richard; BODEAU, Deborah; MCQUAID, Rosalie. **Developing cyber-resilient systems:** a systems security engineering approach. Gaithersburg: National Institute of Standards and Technology, 2021. (NIST Special Publication 800-160, vol. 2, rev. 1). DOI: 10.6028/NIST.SP.800-160v2r1.

ROTHER, Edna Terezinha. Systematic review vs. narrative review. **Acta Paulista de Enfermagem,** São Paulo, v. 20, n. 2, p. v-vi, 2007.

SOPHOS. **The state of ransomware 2024.** Abingdon: Sophos, 2024a.

SOPHOS. **The impact of compromised backups on ransomware outcomes.** Abingdon: Sophos, 2024b.

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: 06/05/2026 | Accepted: 09/06/2026 | Publication: 11/07/2026

STROM, Blake E.; APPLEBAUM, Andy; MILLER, Doug P.; NICKELS, Kathryn C.; PENNINGTON, Adam G.; THOMAS, Cody B. **MITER ATT&CK:** design and philosophy. McLean: The MITER Corporation, 2018.

SWANSON, Marianne; BOWEN, Pauline; PHILLIPS, Amy Wohl; GALLUP, Dean; LYNES, David. **Contingency planning guide for federal information systems.** Gaithersburg: National Institute of Standards and Technology, 2010. (NIST Special Publication 800-34, rev. 1). DOI: 10.6028/NIST.SP.800-34r1.

TØNDEL, Inger Anne; LINE, Maria B.; JAATUN, Martin Gilje. Information security incident management: current practice as reported in the literature. **Computers & Security,** [Amsterdam], v. 45, p. 42-57, 2014.

EUROPEAN UNION. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. **Official Journal of the European Union,** Luxembourg, L 119, p. 1-88, 4 May 2016.

UNITED STATES. Securities and Exchange Commission. **Cybersecurity risk management, strategy, governance, and incident disclosure.** Release no. 33-11216. Washington, DC: SEC, 2023.

VAN DER KLEIJ, Rick; KLEINHUIS, Geert; YOUNG, Heather. Computer security incident response team effectiveness: a needs assessment. **Frontiers in Psychology,** Lausanne, v. 8, art. 2179, 2017. DOI: 10.3389/fpsyg.2017.02179.

VERIZON. **2025 data breach investigations report.** Basking Ridge: Verizon Business, 2025.

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.