Time Management in Cybersecurity Incident Response: A Strategic Framework for Teams and Management

Angel Brenishki, PhD Student
Department of Informatics & Information technology,
University of Ruse "Angel Kanchev"

Rumen Rusev, Assoc.Prof. PhD
Department of Informatics & Information technology,
University of Ruse "Angel Kanchev"

Kameliya Shoylekova, Assoc.Prof. PhD
Department of Informatics & Information technology,
University of Ruse "Angel Kanchev"

Boyana Ivanova, Assist.Prof. PhD
Department of Informatics & Information technology,
University of Ruse "Angel Kanchev"

Abstract: *This study investigates time allocation as a central determinant of incident response effectiveness. Informed by crisis management theory, resilience engineering, and the Observe–Orient–Decide–Act (OODA) Loop decision model, the study reconceptualizes time as a strategic resource rather than a passive constraint, emphasizing decision velocity alongside analytical rigor.*

The paper introduces the Structured Time Management Framework (STMF), an operational framework designed to impose temporal discipline on incident response through defined phases, fixed temporal anchors, mandatory decision checkpoints, and enforced parallel workstreams. STMF was evaluated during live incidents in three organizations over a twelve-month period, demonstrating improved containment speed, regulatory alignment, coordination, and responder confidence.

The findings indicate that organizations achieving effective time allocation consistently limited incident impact and avoided secondary failures, while those with unmanaged temporal drift experienced escalation, regulatory penalties, and reputational harm. The study concludes that disciplined time management is a core strategic capability for modern incident response, delivering both operational and human performance benefits.

Keywords: *incident response, time allocation, crisis management, OODA loop, cybersecurity*

1. INTRODUCTION

The Time Allocation Problem

In practice, incident response (IR) procedures are frequently developed with substantial rigor, yet they are routinely disregarded during live crisis situations. This disconnect arises because most procedural frameworks emphasize *what* actions should be taken, while offering limited guidance on *when* those actions should occur or the duration for which they should reasonably be pursued. As a result, response teams possess task inventories without temporal prioritization, undermining their effectiveness under time pressure.

Evidence from numerous post-incident reviews indicates that response inefficiencies often stem from this temporal ambiguity rather than technical complexity. In several cases, teams reported spending multiple hours deliberating containment strategies while ransomware continued to propagate into backup environments. In others, statutory notification deadlines were missed not due to investigative challenges, but because responsibility for regulatory communication had not been clearly assigned (AYATI, 2025) (MANN, 2025).

These challenges have been exacerbated by the increasing complexity of regulatory environments. While the General Data Protection Regulation (GDPR) introduced a 72-hour notification requirement that appears reasonable in isolation, compliance becomes substantially more difficult when organizations must simultaneously conduct investigation, containment, remediation, and documentation. The Network and Information Security Directive 2 (NIS2) further compresses response timelines through 24-hour reporting obligations, while the Digital Operational Resilience Act (DORA) imposes particularly stringent expectations on financial institutions. Each of these regulatory frameworks has been developed independently, implicitly assuming ideal resource availability and coordination, conditions that rarely exist during real-world incidents (SHAH, 2025).

This study emerged from a persistent discrepancy observed between IR theory and operational practice. Repeated case analyses and interviews with incident responders consistently revealed a common pattern: the availability of strong technical guidance accompanied by significant temporal disorganization during active incidents. One security operations center (SOC) manager characterized this challenge as the presence of comprehensive procedures without corresponding guidance on execution under time pressure, highlighting a systemic gap in operationalization.

This observation points to a fundamental issue in crisis response: the allocation of time is not merely a matter of efficiency, but a determinant of overall effectiveness. Excessively slow responses allow incident impact to escalate, while overly rapid actions increase the likelihood of errors that may exacerbate damage or compromise investigative integrity. Effective incident response therefore requires balancing speed with analytical rigor, and regulatory compliance with evidentiary quality.

Cybersecurity incidents inherently involve multiple, competing priorities. Technical teams require sufficient time for forensic analysis and system restoration; legal and compliance functions must evaluate regulatory obligations; executive leadership depends on timely situational awareness; and communication teams must develop messaging that informs stakeholders without generating undue alarm. Although each function operates under time pressure, these temporal demands are rarely aligned, resulting in fragmented and unsynchronized response efforts (PEKARCIK, 2025).

Research Approach

This research integrates principles from crisis management theory with the operational realities of cybersecurity incident response. Over a two-year period, the study examined five major incidents across multiple sectors, conducted in-depth interviews with fifteen IR professionals, and analyzed regulatory requirements across relevant compliance frameworks (KIANPOUR, 2025).

The distinguishing feature of the approach lies in its analytical focus. The study concentrates on its temporal dimensions - specifically, when actions are initiated and how long they are sustained. Time allocation patterns were systematically compared between successful and unsuccessful incident responses, with particular attention to communication overhead, decision-making latency, and the operational implications of regulatory timelines. Regulatory requirements were examined not solely as legal obligations, but as constraints that actively shape response strategy and execution.

The framework is informed by Boyd’s Observe–Orient–Decide–Act Loop, a decision-making model originating in military aviation that demonstrates strong applicability to dynamic and adversarial cybersecurity environments. A central insight derived from this synthesis is that, in rapidly evolving incidents, decision velocity frequently exerts greater influence on outcomes than decision optimality. The framework is evaluated through deployment in three organizations during live incidents over a twelve-month period. While the results were notable, their implications are presented and analyzed in detail in the following sections (TANUI, 2021).

2. DESIGN OF THE STRATEGIC TIME MANAGEMENT FRAMEWORK

Design Principles

The STMF framework emerged from repeated empirical observation of IR teams whose strong technical competencies proved insufficient under conditions of high operational stress. Across numerous incident engagements, recurring failure modes were observed in teams that otherwise adhered to established response procedures. The STMF was designed explicitly to address these empirically derived deficiencies through five foundational principles.

Figure 1 presents step-by-step implementation of the STMF.

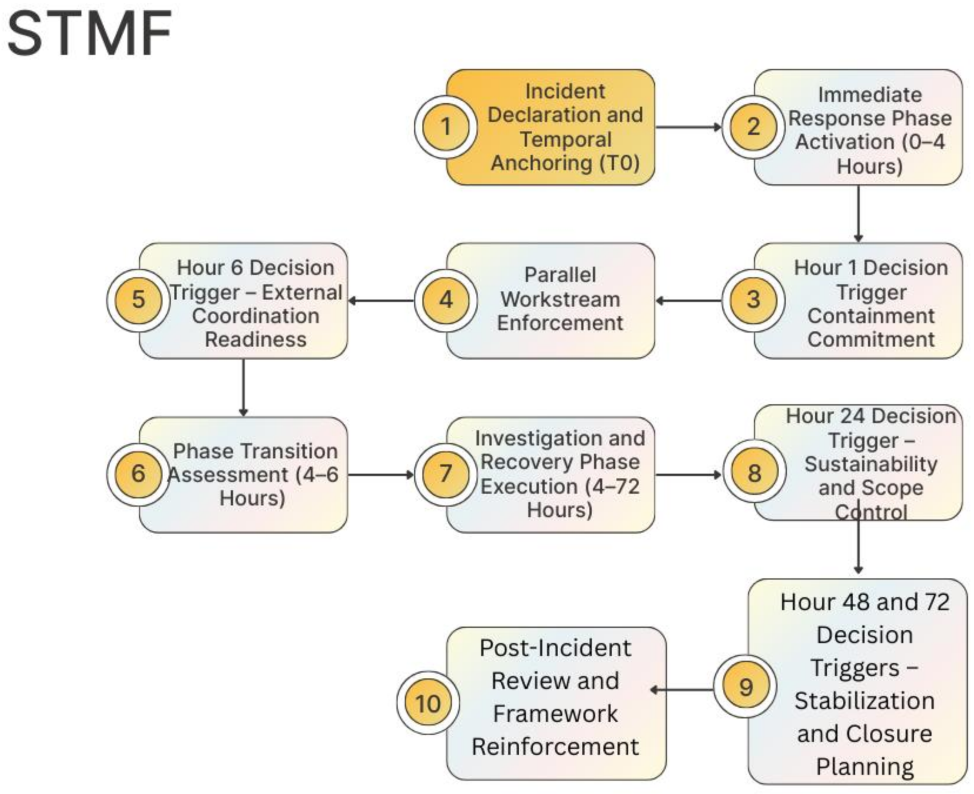
STMF
1
Incident Declaration and Temporal Anchoring (T0)
2
Immediate Response Phase Activation (0–4 Hours)
3
Hour 1 Decision Trigger Containment Commitment
4
Parallel Workstream Enforcement
5
Hour 6 Decision Trigger – External Coordination Readiness
6
Phase Transition Assessment (4–6 Hours)
7
Investigation and Recovery Phase Execution (4–72 Hours)
8
Hour 24 Decision Trigger – Sustainability and Scope Control
9
Hour 48 and 72 Decision Triggers – Stabilization and Closure Planning
10
Post-Incident Review and Framework Reinforcement

Figure 1. STMF Operational Sequence

Step 1: Incident Declaration and Temporal Anchoring (T0)

Upon confirmation of a credible incident, the organization formally declares an incident state and establishes a fixed temporal anchor (T0). All subsequent actions, decision points, and reporting obligations are measured relative to this reference time. Incident command roles are assigned immediately, and scope assumptions are explicitly documented as provisional.

Step 2: Immediate Response Phase Activation (0–4 Hours)

- The Immediate Response Phase is initiated with the primary objective of limiting impact under conditions of uncertainty.
- Establish incident command and role ownership
- Enforce parallel workstreams (containment, investigation, communications, regulatory assessment)
- Document initial hypotheses without requiring validation
- Apply predefined containment actions based on risk thresholds rather than confirmed root cause

This phase prioritizes action over precision, recognizing that early intervention has disproportionate impact on outcome severity.

Step 3: Hour 1 Decision Trigger – Containment Commitment

- At Hour 1, the first mandatory decision checkpoint occurs.
- Determine whether containment actions are sufficient, need escalation, or require modification
- Authorize disruptive actions (e.g., system isolation, credential resets) if risk thresholds are exceeded
- Record decision rationale and unresolved uncertainties
- This checkpoint prevents investigative inertia and ensures early containment momentum.

Step 4: Parallel Workstream Enforcement

- From Hour 1 onward, all response activities proceed in parallel by default:
- Technical track: forensic triage, telemetry expansion, indicator scoping
- Containment track: access restriction, system isolation, control hardening
- Recovery track: backup validation, restoration planning
- Communications track: internal leadership updates, external messaging preparation
- Regulatory track: jurisdictional analysis, notification deadline mapping
- Workstreams are coordinated through incident command but are not allowed to block one another.

Step 5: Hour 6 Decision Trigger – External Coordination Readiness

- At Hour 6, the second decision checkpoint is executed.
- Assess readiness for external communication (customers, partners, regulators)
- Approve preliminary disclosures if notification thresholds may be met
- Adjust containment and investigation priorities based on new intelligence
- This step aligns operational response with legal, reputational, and stakeholder obligations.

Step 6: Phase Transition Assessment (4–6 Hours)

- Between Hours 4 and 6, incident command evaluates transition criteria from Immediate Response to Investigation and Recovery:
- Containment measures are stable or actively reducing risk
- No uncontrolled propagation is observed
- Response tempo is sustainable beyond short-term crisis mode
- If criteria are met, the organization formally transitions phases while maintaining active containment oversight.

Step 7: Investigation and Recovery Phase Execution (4–72 Hours)

- The Investigation and Recovery Phase focuses on root cause analysis, system restoration, and long-term remediation.

- Expand forensic analysis and evidence preservation
- Execute validated recovery plans in controlled increments
- Implement compensating controls and monitoring enhancements
- Continue regulatory and stakeholder engagement as required
- Decision-making remains structured but shifts toward optimization and durability rather than immediacy.

Step 8: Hour 24 Decision Trigger – Sustainability and Scope Control

- At Hour 24, leadership conducts a sustainability review:
- Evaluate personnel fatigue and rotate roles as necessary
- Confirm recovery timelines and residual risk posture
- Decide whether to narrow, expand, or redefine incident scope
- This checkpoint prevents cognitive and operational degradation during prolonged response.

Step 9: Hour 48 and 72 Decision Triggers – Stabilization and Closure Planning

- Subsequent decision checkpoints focus on stabilization and transition to normal operations:
- Validate that recovery objectives are met
- Confirm compliance with all notification and reporting obligations
- Initiate post-incident review planning
- Establish criteria for formal incident closure
- These checkpoints ensure deliberate exit from crisis mode rather than gradual, unmanaged disengagement.

Step 10: Post-Incident Review and Framework Reinforcement

- Following closure, a structured post-incident review is conducted:
- Analyze phase transitions, decision timing, and parallelization effectiveness
- Identify human performance breakdowns and safeguard failures
- Update STMF playbooks, thresholds, and decision criteria accordingly
- The framework is treated as a living operational system, refined through iterative learning.

3. CASE STUDY ANALYSIS

Five security incidents presented in Table 1 were selected for analysis because they collectively illustrate a broad spectrum of time management outcomes, ranging from highly effective response to severe failure.

Table 1. Comparative Summary of Incident Response Cases and Time Allocation Outcomes

Case	Sector / Organization Type	Incident Type	Detection & Initial Response	Key Strengths	Time Allocation (Approx.)	Outcome / Impact
Regional Medical Center	Healthcare (1,200-bed hospital)	Ransomware (WannaCry variant)	Detected via automated monitoring at 14:30; network segmentation within 30 minutes	Pre-configured isolation, rehearsed downtime procedures, parallel task execution, clear authority	Technical: ~65% Communication: ~22% Management: ~13%	Full recovery in 18 hours; minimal operational disruption
Mid-Size Bank	Financial Services	Business Email Compromise	Initially misclassified as routine malware; escalation delayed 48 hours	None notable during early phase	Meetings/Communication: ~45%	96-hour incident; GDPR deadline missed; €25,000 fine; regulatory oversight; reputational damage
Automotive Manufacturer	Manufacturing (OT/IoT)	IoT / OT System Compromise	Detected after unauthorized sensor access	Eventual cross-functional coordination	Asset discovery consumed ~35% of first 24 hours	Mixed outcome; prolonged containment; operational risk mitigated but inefficient response
Retail Chain	Retail (Large-scale)	Payment Card Breach	Detected via automated fraud monitoring; immediate escalation	Rapid containment, parallel forensics and recovery, pre-established vendors, templated communications	Communication: ~18%	Containment within 2 hours; rapid expert engagement; controlled customer impact
Government Agency	Public Sector	Advanced Persistent Threat (APT)	Discovered during security assessment	Deliberate containment, role rotation, separation of technical and political tracks	Coordination/Communication: ~40%	Extended response timeline; response quality maintained

4. CONCLUSIONS

This report concludes that effective IR depends as much on how organizations manage time as on their technical capabilities. Treating time as a strategic, actively managed resource—rather than an uncontrollable constraint—leads to faster response, improved coordination, stronger regulatory compliance, and higher stakeholder confidence.

The Structured Time Management Framework provides a practical, evidence-based approach for achieving these outcomes. By introducing deliberate time allocation, clear decision triggers, and disciplined communication, STMF shifts organizations from reactive crisis behavior to controlled, proactive execution under pressure. This shift reduces escalation risk and prevents incidents from becoming broader organizational crises.

Beyond measurable performance improvements, STMF delivers significant human and cultural benefits. Teams respond with greater confidence, clarity, and resilience, addressing a critical gap in modern IR; the coordination of human decision-making under time pressure. Organizations that adopt STMF develop temporal discipline, a transferable capability that strengthens not only cybersecurity response but overall crisis management and operational resilience.

Finally, the report emphasizes that STMF is immediately actionable and scalable. Incremental adoption using existing structures can yield rapid returns, while long-term benefits include reduced stress, improved morale, and sustained leadership effectiveness during crises. In an increasingly complex threat and regulatory environment, disciplined time management emerges as a core strategic capability and a decisive factor in successful incident response.

REFERENCES

AYATI A., Naji H.R., Hashemi M.M., Saffar M., *Optimizing Location Allocation in Urban Management: A Brief Review*, 2025 29th International Computer Conference, Computer Society of Iran (CSICC), Iran, Islamic Republic of, 2025, pp. 1-7, https://doi.org/10.1109/CSICC65765.2025.10967426

KIANPOUR, M., Frantz., *Analysis of Institutional Design of European Union Cyber Incident and Crisis Management as a Complex Public Good*, Regulation & Governance 19, no. 4: 1037–1062. https://doi.org/10.1111/rego.12640.

MANN, Z.A., *Time is Money: A Temporal Model of Cybersecurity*. Nemec Zlatolas, L., Rannenberg, K., Welzer, T., Garcia-Alfaro, J. (eds) ICT Systems Security and Privacy Protection. SEC 2025. IFIP Advances in Information and Communication Technology, vol 746. Springer, Cham. https://doi.org/10.1007/978-3-031-92886-4_6

PEKARCIK M., Sopko, J., Safar, L., *Cybersecurity in financial institutions: A bibliometric and thematic analysis of global research (2000–2025)*. Veredas Do Direito, 22(7), e223815. https://doi.org/10.18623/rvd.v22.n7.3815

SHAH, I. H., *Digital Operational Resilience Act (DORA) And Similar Global ICT Risk Management Frameworks Requires a Structured Approach That Balances Theory, Empirical Evidence, And Critical Analysis*, http://dx.doi.org/10.2139/ssrn.5391781

TANUI D. J., Application of Boyd's OODA Loop to Emergency Response. Journal of Emergency Management, vol. 19, no. 5, Sept. 2021, pp. 461-8, doi:10.5055/jem.0564.