The Four Battles™ of Cyber Incident Response

A Leadership Framework for Containing Damage, Preserving Operations, Meeting Legal Duty, and Protecting Trust

Scott Foote

Last Updated: 27 March 2026

Phenomenati Consulting
www.phenomenati.com

6 Liberty Square, #2736
Boston, MA 02109
(508) 709-7990 (office)

<this page is intentionally blank>

Contents

1 Executive Summary

Core Thesis: After multiple decades designing, building, deploying, operating, and defending business-critical information systems, I have come to a simple conclusion: a serious cyber incident is never just ***one*** fight. It becomes ***four*** simultaneous battles... *technical*, *operational*, *legal*, and *reputational*... and the enterprise only wins when it leads all four together.

Caveat: This paper is a leadership framework, not legal advice. Actual disclosure and notification duties vary by jurisdiction, sector, contract, insurance policy, and the facts of the event.

How does your organization want to be perceived after a cyberattack, a resulting compromise, and the possible exposure of sensitive stakeholder information: as the ***Victim*** or the ***Villain***? In today's environment, even well-run enterprises can fall prey to sophisticated, persistent, and well-funded adversaries. Boards, regulators, customers, patients, partners, investors, and the public generally understand that no organization is immune. What they judge... often immediately and unforgivingly... is not simply whether you were attacked, but whether you were ***prepared***, whether you ***responded with discipline*** and ***urgency***, and whether you ***protected*** the people who trusted you with their data.

An organization becomes the ***villain*** not because it was targeted, but because it appears ***careless***, ***evasive***, ***disorganized***, or ***indifferent*** in the moments that matter most. *Delay, denial, weak coordination, poor legal judgment, operational chaos*, and *tone-deaf communications* can turn a criminal act committed against the enterprise into a leadership failure attributed to it. That is why cyber incident response is never just a technical exercise. It is a defining enterprise event fought across four simultaneous fronts: ***technical***, ***operational***, ***legal***, and ***reputational***. The organizations that emerge with trust intact are those that understand this early, lead decisively, and respond in a way that is competent, transparent, and worthy of stakeholder confidence.

Critical in this phenomena, most organizations still frame cyber incidents too narrowly. They treat the event as a technical compromise to be remediated by security and IT. That view is incomplete. A major incident immediately becomes the four simultaneous battles: a technical battle to contain and recover, an operational battle to keep the enterprise functioning, a legal battle to satisfy obligations and manage liability, and a reputational battle to preserve stakeholder trust. Modern guidance increasingly treats incident response as part of enterprise risk management and organizational resilience rather than a narrow SOC or IT operations activity [1][2][3].

The Four Battles™ phenomenon matters because each battle runs on a ***different clock*** and optimizes for a ***different outcome***. The *technical* battle is measured in minutes and hours. The *operational* battle is measured in service continuity and business impact. The *legal* battle is measured against statutory, regulatory, contractual, and evidentiary deadlines. The *reputational* battle starts almost immediately and can last months or years because customers, regulators, partners, investors, and the media will judge not just what happened, but how the organization behaved. Guidance from NIST, CISA, ISO, the SEC, HHS, and European regulators all point in the same direction: preparedness, leadership clarity, stakeholder communication, and disciplined recovery determine whether an incident becomes a contained event or a prolonged crisis [1][3][4][5][6][7][8][9][10].

Working premise. The organization ***wins*** the incident only when it can stop the adversary, continue priority operations, meet legal duties, and preserve trust at the same time.

Exhibit 1. The Four Battles at a Glance

Battle	Led By	Primary Objective	Primary Clock	Primary Outputs
Technical	CISO and CIO teams	***Contain*** the intrusion, ***eradicate*** malicious activity, ***restore*** systems, and ***prevent*** further spread	Minutes to days	Triage, isolation, forensics, patching, credential rotation, restoration
Operational	Business and Operations Leadership	Keep ***mission-critical services*** running while technology is unstable	Hours to weeks	Manual workarounds, service prioritization, rerouting, downtime management
Legal	General Counsel and Compliance	Preserve ***privilege***, satisfy ***notice obligations***, protect ***evidentiary*** and ***liability*** posture	Immediate to statutory deadlines	Regulatory analysis, hold notices, disclosures, contractual response
Reputational	Marketing, Communications, and Legal	Protect ***confidence*** among customers, regulators, partners, investors, employees, and media	Immediate to months/years	Holding statements, FAQs, stakeholder updates, media and investor messaging

*Each battle has a different leader, tempo, success metric, and decision logic. The **executive failure mode** is to let one battle dominate while the others go unmanaged.*

2 Battle One: the *Technical* Battle

LEAD	PRIMARY CLOCK	WIN CONDITION
the CISO and CIO teams	Minutes to days	Threat contained and systems restored safely

The technical battle is led by the CISO and CIO teams because containment without restoration is not victory, and restoration without security is not recovery. The immediate fight is to identify the intrusion, understand the ***blast radius***, contain the adversary, preserve evidence, eradicate persistence, patch or mitigate exploited weaknesses, and restore systems safely. NIST's current incident response guidance explicitly places response and recovery within the broader context of cyber risk management and improvement, while CISA's ransomware guidance emphasizes detection, prevention, response, and recovery as a unified discipline [1][4].

Under extreme pressure and extreme scrutiny, this team must make ***decisions*** *with incomplete facts*: whether to isolate segments, disable accounts, take systems offline, rotate credentials, invoke disaster recovery, or rebuild from known-good images. These actions can be *technically correct* and *operationally painful* at the same time. That is why the technical battle must report both security *facts* and *business implications*, not just indicators of compromise.

In mature organizations, the technical battle also guards against the false comfort of premature restoration. A system that is back online but still exposed, still untrusted, or still missing identity integrity is not truly recovered. The standard must be *safe* restoration, not merely fast restart [1][4].

2.1 What Good Looks Like

INDICATORS OF CONTROL

- Incident ***severity*** declared quickly and a technical commander established
- ***Blast radius***, affected identities, and priority containment actions understood
- ***Evidence*** preserved before destructive remediation or rebuild activity
- ***Backups***, credential ***integrity***, and *restoration* paths verified as trustworthy
- ***Re-entry criteria*** defined before reconnecting recovered systems

EXECUTIVE QUESTIONS

- What do we know, what do we suspect, and what are we doing in the next four hours?
- Which identities, systems, data stores, and third parties are in scope?
- What is the safest path to restore operations without reintroducing the threat?

3 Battle Two: the *Operational* Battle

Led by business and operations leadership

LEAD	PRIMARY CLOCK	WIN CONDITION
business and operations leadership	Hours to weeks	Critical services continue acceptably

While the technical teams fight the adversary, business and operations leaders fight for ***continuity***. Their objective is not to pretend nothing happened; it is to ***preserve*** **mission-essential** ***output*** while the environment is unstable. In clinical, financial, manufacturing, and customer-facing environments, that can mean rerouting workflows, reverting to manual processes, prioritizing critical services, or deliberately reducing service levels to keep the enterprise viable. ISO 22301 and the NIST Cybersecurity Framework both frame ***resilience*** as the ability to plan for, absorb, and recover from disruption, which makes the operational battle inseparable from cyber response [2][3][6].

The operational battle decides what the enterprise *must keep doing* at all costs, what can *pause*, what can *degrade gracefully*, and where scarce capacity should be directed. Mature organizations do not wait for perfect forensic certainty before making continuity decisions; they use pre-defined business impact analysis, recovery objectives, manual workarounds, and alternate suppliers or sites when available.

This is where cyber response becomes unmistakably a ***business*** discipline. Security teams may stop the attacker, but business leaders determine whether the organization can still serve patients, ship products, settle transactions, deliver payroll, or keep customers informed while technology is impaired.

3.1 What Good Looks Like

INDICATORS OF CONTROL

- ***Critical services prioritized*** for the next 24, 72, and 168 hours
- ***Manual workarounds*** and fallback procedures are safe, legal, and sustainable
- Service ***degradation thresholds*** and *shutdown decisions* are explicit
- Customer, safety, revenue, and compliance ***tradeoffs*** are documented
- Line-of-*business* leaders own continuity decisions, not just IT

EXECUTIVE QUESTIONS

- What business services cannot fail?
- Which workarounds are safe, legal, and sustainable for more than a few hours?
- What losses are we preventing by acting now, even if full recovery is incomplete?

4 Battle Three: the *Legal* Battle

Led by General Counsel and Compliance

LEAD	PRIMARY CLOCK	WIN CONDITION
General Counsel and Compliance	Immediate to deadline	Obligations met and posture protected

Simultaneously, the General Counsel and Compliance leaders enter a race against multiple clocks. Their task is to ***establish privilege*** where appropriate, direct or coordinate ***investigations***, preserve ***evidence***, assess ***legal exposure***, interpret sector-specific ***obligations***, manage outside counsel and forensic vendors, and determine ***who*** must be notified, ***when***, and on ***what*** basis.

The complexity is not theoretical. U.S. public companies may have **Form 8-K obligations** within four **business days** after determining a cybersecurity incident is material [7]. **GDPR Article 33** generally requires notice to a supervisory authority **within 72 hours** for notifiable personal data breaches [8]. **HIPAA** breach notification rules impose ***separate*** notice requirements, including deadlines no later than **60 days** *from discovery* for certain notices [9]. Covered entities under the **EU's NIS2 regime** face a staged model of ***24-hour* early warning**, ***72-hour* notification**, and a final report ***within one month*** [10].

Legal teams therefore *cannot* be downstream spectators waiting for the forensic report to finish. They must shape the investigation from the beginning because the quality of evidence preservation, documentation, and decision records can materially affect privilege, regulatory outcomes, contractual disputes, insurance recovery, and litigation posture. The legal battle is not won by saying less; it is won by saying the *right things*, at the *right time*, to the *right audiences*, with *defensible records*.

4.1 What Good Looks Like

INDICATORS OF CONTROL

- Privilege and external-counsel ***strategy*** established early where appropriate
- Jurisdictional, contractual, and sectoral ***notification matrix*** activated
- Evidence ***preservation***, ***legal holds***, and ***chain-of-custody*** maintained
- Disclosure and materiality decisions supported by disciplined records
- Regulatory, insurer, and law-enforcement ***interfaces*** coordinated

EXECUTIVE QUESTIONS

- Which legal and regulatory clocks are already running?
- What facts do we need before a disclosure or notification decision is made?
- What evidence must be preserved before systems are rebuilt, wiped, or returned to service?

5 Battle Four: the *Reputational* Battle

Led by Marketing, Communications, and Legal

LEAD	PRIMARY CLOCK	WIN CONDITION
Marketing, Communications, and Legal	Immediate to long-tail	Stakeholder confidence preserved

The reputational battle is ***often the last*** to be acknowledged and the longest to end. Stakeholders rarely judge an organization solely by the existence of an incident; they judge whether leadership was ***candid***, ***organized***, ***empathetic***, and ***competent***. NIST guidance emphasizes that *meaningful* coordination and communication with stakeholders improves response and mitigation, while CISA guidance stresses stakeholder planning and contingencies in the event ordinary internal communications channels are unavailable [3][5].

This battle is ***not*** public relations spin. It is the *disciplined management* of ***trust***. Communications must be transparent enough to be ***credible***, careful enough to be ***legally sound***, and frequent enough to ***prevent rumor*** from becoming the dominant narrative. Customers want practical guidance. Regulators want timely, accurate statements. Employees want clarity. Partners want operational certainty. Investors want to understand material impact and management control. The media will interpret *silence* as *confusion* unless there is a deliberate holding statement and update cadence.

In practice, this means communications teams, legal counsel, investor relations, customer leadership, HR, and executive leadership must coordinate around ***one fact base*** and ***one message architecture***. Message *discipline* is not about uniformity for its own sake; it is about ensuring that every stakeholder hears a truthful, useful, and defensible version of the ***same*** **reality**.

5.1 What Good Looks Like

INDICATORS OF CONTROL

- ***Holding statement*** and audience-specific ***message tracks*** are ready quickly
- ***Single source of truth*** exists for facts, assumptions, and approved language
- Customer, regulator, partner, investor, and employee ***messaging*** is *synchronized*
- ***Rumor control*** and ***correction*** are active across media and social channels
- Leadership demonstrates ***responsibility***, ***empathy***, and ***control***

EXECUTIVE QUESTIONS

- Who needs to hear from us next, and what do they need to know now?
- What can we state with confidence today, and what must wait for confirmation?
- How are we demonstrating responsibility, empathy, and operational control?

6 Winning the Incident: *One* War, *Four* Concurrent Battles

Organizations do not fail incident response only because the adversary was sophisticated. They fail because each battle ***optimizes locally*** and ***conflicts globally***. The technical team wants to isolate aggressively; operations wants systems kept alive; legal wants precision and evidence; communications wants speed and clarity. Executives need an ***integrated command model*** that reconciles these *natural tensions* without paralyzing action [1][5].

The most effective operating model is straightforward: **one *executive incident commander***, **four *designated battle leads***, **one *common operating picture***, **one *decision log***, **one *out-of-band communications plan***, and **one *predictable battle rhythm*** for briefings, decisions, disclosures, and stakeholder updates. Recovery must be defined broadly enough to include safe restoration, evidentiary integrity, legal completion, and trust repair; not merely the moment systems return to service [1][3][5].

Exhibit 2. Typical Tensions Across the Four Battles

Decision point	Technical	Operational	Legal	Reputational
Network Isolation	Stop spread immediately	Maintain essential service	Preserve evidence and approvals	Explain outage honestly
Restoration Timing	Rebuild only when safe	Resume mission now	Retain records and preserve chain-of-custody	Set realistic expectations
Initial External Statement	Avoid speculation	Provide service guidance	Avoid inaccurate or prejudicial language	Show accountability and empathy

6.1 Five Operating Principles

- **One executive incident commander**. One leader owns decision integration, escalation, and priority setting across all four battles.
- **Four designated battle leads**. The CISO/CIO, business operations, general counsel/compliance, and communications/legal functions should each have named primaries and alternates.
- **One Common Operating Picture**. Maintain a disciplined fact base separating confirmed facts, working hypotheses, business impacts, deadlines, decisions taken, and open questions.
- **One Battle Rhythm**. Establish a predictable cadence for technical briefings, executive decisions, regulatory reviews, and stakeholder communications... even when internal collaboration tools are impaired [5].
- **One Definition of Recovery**. Recovery is complete only when the technical, operational, legal, and reputational dimensions have all reached an acceptable end state [1][3][7][8][9][10].

7 Conclusion

On the subject of ***Victim*** or ***Villain***… if I could institutionalize only one idea in every boardroom and executive war room, it would be this: a cyber incident is not ***one*** battle with support functions around it. It is ***four*** *concurrent* battles with different leaders, different clocks, and different definitions of success. The organization that recognizes this early will coordinate faster, communicate better, and recover with less damage. The organization that sees only the technical fight may restore systems and still lose the business.

The next tabletop exercise should not simply ***test the SOC***. It should ***test the enterprise***. Run **one scenario**, **four battle leads**, **one executive commander**, and **one common clock**. Measure not only containment speed, but operational endurance, legal timeliness, and stakeholder confidence. That is how organizations build resilience at scale.

8 References

[1] Nelson, A., Rekhi, S., Scarfone, K., and Souppaya, M. Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile (NIST SP 800-61r3). National Institute of Standards and Technology, Apr. 3, 2025. https://doi.org/10.6028/NIST.SP.800-61r3

[2] National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29). Feb. 26, 2024. https://doi.org/10.6028/NIST.CSWP.29

[3] National Institute of Standards and Technology. NIST Cybersecurity Framework 2.0: Resource and Overview Guide (NIST SP 1299). Feb. 26, 2024. https://doi.org/10.6028/NIST.SP.1299

[4] Cybersecurity and Infrastructure Security Agency. StopRansomware Guide. Oct. 19, 2023. https://www.cisa.gov/resources-tools/resources/stopransomware-guide

[5] Cybersecurity and Infrastructure Security Agency. Incident Response Plan (IRP) Basics. Jan. 31, 2024. https://www.cisa.gov/sites/default/files/publications/Incident-Response-Plan-Basics_508c.pdf

[6] International Organization for Standardization. ISO 22301:2019 Security and resilience ... Business continuity management systems ... Requirements. 2019. https://www.iso.org/standard/75106.html

[7] U.S. Securities and Exchange Commission. Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure: A Small Entity Compliance Guide. Aug. 30, 2023. https://www.sec.gov/resources-small-businesses/small-business-compliance-guides/cybersecurity-risk-management-strategy-governance-incident-disclosure

[8] Regulation (EU) 2016/679 (General Data Protection Regulation), Art. 33. Official Journal of the European Union, 2016. https://eur-lex.europa.eu/eli/reg/2016/679/oj

[9] U.S. Department of Health and Human Services, Office for Civil Rights. Breach Notification Rule. https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

[10] European Commission. Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive) – FAQs. Jun. 29, 2023. https://digital-strategy.ec.europa.eu/en/faqs/directive-measures-high-common-level-cybersecurity-across-union-nis2-directive-faqs