# Calling Out a Cyber Crisis: A Typology for Cyber Incident and Crisis Management

**Katariina Hujanen**
Leiden University
k.s.hujanen@fgga.leidenuniv.nl

**Jeroen Wolbers**
Leiden University
j.j.wolbers@fgga.leidenuniv.nl

**Bibi van den Berg**
Leiden University
b.van.den.berg@fgga.leidenuniv.nl

**ABSTRACT**

Only a subset of cyber incidents in organizations escalates into a full-blown cyber crisis that overwhelms technical response capacities and has severe societal consequences. We clarify the transition from incident to crisis management and conceptualize escalation as a sociotechnical process shaped by sensemaking, decision-making, and multi-actor coordination. To do so, we synthesize cyber incident and cyber crisis management literature and propose a typology to illustrate the pressures and turning points in this transition based on actual cases. We discuss implications for preparedness, incident management, sensemaking, and post-incident learning that integrates technical remediation with crisis leadership and communication.

**Keywords**

Cybersecurity, Incident Management, Crisis Management, Digital Technology, Cyber Crisis

## INTRODUCTION

In the past decades, private and public organizations have become increasingly dependent on digital technologies, so much so that Laura DeNardis argues that by now every company has become an IT company (DeNardis, 2020). Digital technologies form the backbone for production processes, communication with suppliers and customers, service management and delivery, logistics, and finance. When these technologies are disrupted either because of an attack or an outage, business continuity is at stake (Phillips & Tanner, 2019). For many organizations, cyber incidents have become a routine operational reality, where security operations centers (SOCs) and incident response teams handle a continuous flow of alerts, ranging from phishing emails and routine malware detections to irregular network traffic, configuration anomalies, and failed authentication attempts (Vielberth et al., 2020).

Most cybersecurity incidents do not escalate into full-blown crises but remain manageable everyday digital events. When these events, however, surpass the routine, they can trigger significant operational, political, or societal effects. Several well-documented cases illustrate the scale and disruptive potential of high-impact attacks. The 2017 WannaCry ransomware outbreak, for example, compromised hundreds of thousands of systems in over 150 countries and caused major operational disruptions in healthcare and transportation sectors (Lee et al., 2017). That same year, the NotPetya malware campaign spread rapidly through global businesses, with estimates suggesting more than 2,300 affected organizations worldwide (Kaspersky, 2017). Among the most severely hit was Maersk, where the attack disabled approximately 4,000 servers and 45,000 computers across its global operations (Wired, 2018). Equally, accidents in cyberspace can also cause severe damage. In 2024, CrowdStrike released a faulty update on Microsoft Windows systems that caused around 8.5 million computers across many sectors to crash and fail to restart properly (Mugu et al., 2024).

Understanding what it takes when a cyber incident escalates into a crisis is a pressing question. This matters because such escalation is not merely a matter of incident severity but asks organizations to activate their crisis

mode. This shift involves organizational sensemaking, decision-making under uncertainty, and the ability to mobilize appropriate response structures (Wolbers et al., 2025). It forwards the question: do organizations need fundamentally different capabilities to manage a cyber crisis, or does the existing repertoire for incident management suffice? The answer has implications for how organizations invest in preparedness, design crisis response structures, and train key personnel. Without clarity on escalation processes, organizations risk underreacting or overreacting during cyber events with potentially serious consequences.

Current scholarship offers limited conceptual clarity when a cyber incident becomes a crisis. In many articles, the terms cyber incident and cyber crisis appear to be used interchangeably (Prevezianou, 2021). Few studies have explicitly noted the boundary between incidents and crises (Ruohonen et al., 2025). Prevezianou (2021) for instance, notes that *"even the cases that do present all the characteristics that would classify them as crises"* are often not labelled as such (p. 55). This results in a persistent 'gray area' in how events are defined, categorized, and ultimately governed. The WannaCry ransomware attack is illustrative of this: it was framed as a crisis in the United Kingdom due to its disruption of the National Health Service (Lee et al., 2017), yet it was not elevated to a crisis status by the EU, illustrating how the same event can be differently labeled across governance levels and institutional contexts (ENISA, 2024). The lack of shared language and criteria complicates practice: failing to recognize escalation can delay critical interventions and jeopardize essential services, yet prematurely declaring a crisis may activate costly or disruptive measures, harm organizational reputation, or trigger unnecessary reactions from partners and the public.

To advance both conceptual clarity and practical guidance, we need a better understanding of how transitions from incidents to crises unfold and what internal and external pressures influence organizations. This requires examining escalation as a temporal process: how initial signals are interpreted, how organizations scale their response, and how decision thresholds are negotiated in real-time. Against these thoughts, we ask: When do organizations shift from incident to crisis management and what pressures do they face in this process? As a starting point of a 5-year PhD project examining when and how cyber incidents escalate to cyber crises, this paper introduces a preliminary typology of the pressures that organizations may encounter when cyber incidents escalate to cyber crises.

## CYBER INCIDENT MANAGEMENT

For larger and digitally mature organizations, cyber incident management forms a core component of the cybersecurity strategy and part of a larger set of coordinated actions to prevent, detect, analyze, and respond to incidents (Onwubiko & Ouazzane, 2020; Tøndel et al., 2014). Cyber incidents vary widely in nature and severity, but are broadly defined as an incident that "leads to, or […] could reasonably lead to …(1) a substantial loss of confidentiality, integrity, or availability of a covered information system, network, or operational technology; (2) a disruption or significant adverse impact on the covered entity's ability to engage in business operations or deliver goods, or services, including those that have a potential for significant impact on public health or safety or may cause serious injury or death; (3) disclosure or unauthorized access directly or indirectly to non-public personal information of a significant number of individuals; or (4) potential operational disruption to other critical infrastructure systems or assets." (Department of Homeland Security, 2023, p. 26). Over the past decades, incident management has matured into an established organizational practice supported by widely adopted international standards and industry frameworks (He et al., 2022). These frameworks, published by for example the International Organization for Standardization (ISO) and the National Institute of Standards and Technology (NIST), provide input for various approaches to incident management (Tøndel et al., 2014; Nelson et al., 2025). Most standards converge on a set of core practices known as the incident response lifecycle, typically comprising preparation; detection and analysis; containment, eradication, and recovery; and post-incident activity (Cichonski, 2012; Vielberth et al., 2020).

### *Preparation*

Preparing for cybersecurity incidents requires the monitoring of networks, devices and traffic and extensive data collection. Organizations aggregate and process large volumes of security logs and telemetry from diverse systems, applications, and network nodes (Madani et al., 2011). Analysts and automated systems work to normalize, filter, and correlate this data to reduce noise and improve the signal quality needed for detection (Vielberth et al., 2020). Maintaining this data infrastructure represents a substantial portion of preparedness.

### *Detection and analysis*

Detection involves transforming raw data into actionable intelligence. Organizations rely on a combination of automated alerts and human interpretation, including employees reporting phishing attempts (Vielberth et al.,

2020). During a triage analysts classify alerts, distinguish benign anomalies from genuine threats, and escalate potentially harmful incidents. This work is labor-intensive, requiring advanced technical and organizational knowledge. Although tools such as Security Information and Event Management (SIEM) systems, intrusion detection systems (IDS), and automated correlation engines (Lakshmi et al., 2021; Bhatt et al., 2025), analysts frequently encounter alert fatigue, false positives, and incomplete or ambiguous data.

#### *Containment, eradication, and recovery*

Once an incident is validated, responsibility shifts to incident response teams, consisting of technical specialists and system owners that isolate affected assets, remove malicious artifacts, and restore system integrity to return to normal operations. During ransomware attacks, negotiation experts are also included in these teams. Automation is increasingly used to accelerate containment, including isolating endpoints, blocking malicious traffic, or deploying patches (Vielberth et al., 2020).

The literature indicates this work is largely structured by incident severity. Low-impact events follow standardized procedures, while high-impact incidents require coordination across technical and business units for impact assessment (Ahmad et al., 2012). In mature organizations, impact assessments follow formalized criteria, and high-impact incidents involve extensive operational knowledge gathering across technical and non-technical domains. Overall, incident response demands cross-functional coordination, rapid decision-making, and negotiation between cybersecurity teams, IT operations, and business units, particularly for severe incidents.

#### *Post-incident activity*

The final phase of incident management focuses on drawing lessons-learned, improving policies, and adapting technical controls. Despite its importance, organizations frequently underinvest in post-incident learning in favor of operational demands (He et al., 2022). As a result, incident response often remains reactive, and recurring vulnerabilities and bottlenecks persist.

### Organizational Structures for Cyber Incident Management

Building on the understanding of cyber incident management as a structured organizational practice, we briefly touch upon the institutional arrangements through which it operates. Notably such a structured organizational practice only exists in larger, digitally mature organizations; smaller or less mature organizations often outsource this function or lack it entirely.

In organizations with structured cyber incident management, this function is embedded in a multi-layered organizational ecosystem of operational monitoring units, specialized response teams, and, at higher levels, sectoral and/or national coordination bodies. Although this division of labor is widely recognized in practitioner and academic communities, the terminology and boundaries between these units remain fluid. Labels such as Security Operations Centers (SOC), computer emergency response teams (CERT), and cyber security incident response teams (CSIRT) are defined inconsistently across organizations and regulatory frameworks. A brief clarification of these organizational forms is therefore necessary.

#### *Security Operations Centers (SOCs)*

At the organizational level, day-to-day monitoring and detection are concentrated in Security Operations Centers (SOCs), which serve as frontline units within sectors such as technology, finance, and government (Tariq et al., 2025). SOCs operate in high-stakes environments requiring continuous vigilance and timely escalation of threats (Onwubiko & Ouazzane, 2020). A persistent is alert fatigue, caused by high event volumes and constant triage demands (Tariq et al., 2025), prompting research focused on efficiency and workload reduction.

SOCs differ in structure and maturity levels. Workflows reflect organizational priorities, budgets, sectoral regulation, but also the type of technology used (Sundaramurthy et al., 2014; Vielberth et al., 2020). Larger organizations often adopt hierarchical, tiered models in which junior analysts follow standardized playbooks and escalate cases to more experienced staff (Vielberth et al., 2020; Onwubiko & Ouazzane, 2020). Smaller SOCs typically have flatter structures with broader analyst roles and less formal specialization (Sundaramurthy et al., 2014).

*Incident response*

When incidents exceed routine handling, responsibility shifts to specialized incident response teams, either permanent or more ad-hoc units within an organization, that manage the technical and organizational response. Sometimes these teams are called Computer Emergency Response Teams (CERTs), at other times Cybersecurity Incident Response Teams (CSIRTs). Confusingly, terminology becomes ambiguous at the supra-organizational level, where sectoral or national bodies may also be designated CERTs or CSIRTs. These entities coordinate large-scale incident response, facilitate sectoral information sharing on threats, risks and best practices, and provide guidance on strengthening sectoral organizational cybersecurity maturity. Under the European NIS2 Directive, the term CSIRT is now reserved exclusively for sectoral or national level units.

Studies show response teams may encompass diverse roles and functions. Brown et al. (2016) identify core functions including incident coordinator, technical responders, and communication staff, with additional personnel engaged during large-scale incidents. These roles underscore that incident response is not merely a technical activity, but necessitates coordination, collaboration, judgment, and shared decision-making between actors. These teams may also engage in proactive efforts to test the resilience of their cybersecurity through vulnerability assessments or penetration testing (Ahmad et al., 2012). We do note that the organizational arrangements in which incident response teams operate vary. They may operate as standalone units, be embedded within SOCs, or outsourced to external providers (Cichonski et al., 2012). While organizational and cognitive dimensions are a key part of incident response, they receive comparatively little attention in the literature, as it disproportionately focuses on technical processes (Vielberth et al., 2020). Consequently, critical challenges related to governance, leadership, communication, and organizational learning remain relatively underexplored.

## CYBER CRISIS MANAGEMENT

Whereas incident management concerns the structured operational handling of routine or acute cybersecurity events that organizations can contain or resolve, crisis management is required to the type of cybersecurity events that escalate beyond technical containment and create broader societal, organizational, or political disruption (van den Berg & Kuipers, 2022). In recent years, cyber crises have featured in European policy discourse, national preparedness strategies and EU-level plans for large-scale digital disruptions. In academic literature, cyber crises are commonly conceptualized as a subset of transboundary crises: crises whose causes, impacts, and responsibilities stretch across organizational, sectoral, and territorial boundaries (Prevezianou, 2021; Backman, 2021). Cyber crises are characterized by their speed, opacity, and interconnectedness, often involving cascading technical failures, cross-border digital infrastructures, and interdependencies that complicate attribution and coordination. Compared with 'traditional' crises (e.g., industrial accidents or natural hazards), cyber crises exhibit invisible causes and non-linear escalation patterns, making early recognition and a targeted response difficult.

Classical crisis definitions help clarify the conceptual distinction between incidents and crises. Crises are defined as a serious threat to the basic structures or the fundamental values and norms of a system, which, under time pressure and highly uncertain circumstances, necessitate vital decision-making (Rosenthal et al., 1989). Pearson and Clair (1998) focus on organizations, and describe crises as low-probability, high-impact events that threaten organizational survival and must be managed under intense time pressure. Kuipers and Wolbers (2021) similarly characterize organizational crises as acute disruptions to core processes that demand an immediate and strategic response. In contrast to incidents, which may involve high urgency but are managed and contained by established protocols and procedures, the defining feature of a crisis is the coexistence of urgency and fundamental uncertainty about appropriate action. In cyber contexts, this uncertainty arises from incomplete situational awareness, complex attack vectors, and ambiguity about the extent of compromise or potential cascading effects across interconnected systems (Vielberth et al., 2020).

Two conceptual refinements from crisis research are important to understand the dynamics of cyber crises. First, Roux-Dufort's (2007) distinction between event-centric and processual views offers an important lens. In the event-centric perspective, crises appear as sudden ruptures requiring immediate intervention. This perspective is often not helpful in understanding the origin of an organizational crisis. Instead, the processual view emphasizes crises as the culmination of long-term vulnerabilities, unnoticed warning signals, and organizational blind spots. From this processual perspective, cyber crises may emerge from enduring deficiencies, such as unpatched systems, technical debt, dependency on legacy systems, or insufficient monitoring, that are activated by a triggering event. The progression from warning signals to acute disruption follows patterns like classic crisis trajectories described by Turner (1976) and Pearson and Mitroff (1993). Crucially, Roux-Dufort (2007) differentiates between urgency and crisis: urgency occurs when solutions are known but time is scarce; crisis emerges when both time and clarity about viable solutions are lacking. This framing provides a conceptual anchor for distinguishing cyber incidents from cyber crises: escalation occurs when established incident response norms no longer suffice, and uncertainty about appropriate action becomes dominant.

Second, the leading social constructivist perspective on crisis occurrence teaches us that crises are not solely objective events but should be regarded as interpretive phenomena shaped through interaction, framing, and meaning-making (Boin et al., 2017). Similarly, based on a review of crisis communication literature, Kuipers et al. (2023) show that crises gain legitimacy through narrative construction and negotiated interpretations among actors. In cyber contexts, this implies that an incident becomes a crisis not only because of its technical characteristics, but because key actors (government agencies, regulators, media, or the public) frame it as such. Such crisis claims are important, as a crisis status affects the mobilization of resources, activation of emergency structures, and public communication strategies. Thus, cyber crisis management is not just a technical endeavor; it involves both material and symbolic dimensions (van den Berg & Kuipers, 2022).

## TOWARDS A TYPOLOGY FOR NAVIGATING CYBER INCIDENT AND CRISIS MANAGEMENT

Cyber crisis management requires the integration of technical remediation with organizational leadership, governance, and communication. Although its triggers may be technical, consequences span people, teams, supply chains, interorganizational relations and affect public trust. Effective cyber crisis management therefore requires executive oversight, clear decision-making authority, and cross-departmental coordination. It also demands strategic communication with internal staff, customers, regulators, and, in some cases, national authorities. Technical containment efforts must be coupled with organizational sensemaking, stakeholder engagement, and transparent messaging to manage uncertainty and restore legitimacy. As such, cyber crisis management requires a hybrid response capacity that treats cybersecurity disruptions not merely as IT problems but as company-wide efforts with potentially severe societal implications.

Yet, integrating technical remediation efforts with broader organizational capacities remains a persistent challenge. Organizations are generally reluctant to activate their crisis mode, partly because doing so disrupts routine operations and requires senior leadership attention, but also because it implies acknowledging a loss of control. We know from crisis literature that switching from incident management to crisis management practices is hard, as organizations need a very different mindset, capabilities and resources (Schakel et al., 2016; Schakel and Wolbers, 2021). It requires different actors to step in, such as executive leaders, communication specialists, business continuity teams, or external cyber crisis management teams, each of whom may not be part of the everyday incident response structure.

Complicating matters further is the fact that the boundary between an ‘incident’ and a ‘crisis’ is rarely clear-cut. Escalation is not solely a function of technical severity of an incident as discussed; it is socially constructed by organizational perceptions, situational framing, and the anticipated consequences for operations, reputation, or legal obligations. As a result, someone within the organization must explicitly declare that the situation has crossed a threshold that warrants a crisis-level response. This decision is both analytical and interpretive: it requires assessing uncertain information, considering interdependencies, recognizing emerging risks, and acknowledging that existing routines may no longer suffice.

This process, while challenging in conventional crisis environments, is further obfuscated in cyberspace. Factors like lacking visibility into systems, technical complexity, ambiguity of impact, distributed ownership of infrastructure, and asynchronous propagation of effects make it difficult to establish a shared, real-time understanding of what is happening. Information may be fragmented across specialized teams, interpreting signals through domain-specific lenses, making it harder to determine when escalation is justified and to align stakeholders around a unified framing (Wolbers, 2022).

Consequently, organizations navigating the unfolding escalation may face different internal and external pressures when deciding whether to call out a crisis. Delays or hesitation in making this call can exacerbate the impact of the incident, while premature escalation may strain resources unnecessarily, or lead to significant economic or reputational costs. The challenge, therefore, lies in managing the technical aspects of cyber incidents, while navigating the organizational, cognitive, and procedural pressures inherent in declaring a crisis. To conceptually navigate the different pressures surrounding this process, we have constructed a preliminary typology illustrating the different types of pressures organizations might be confronted with.

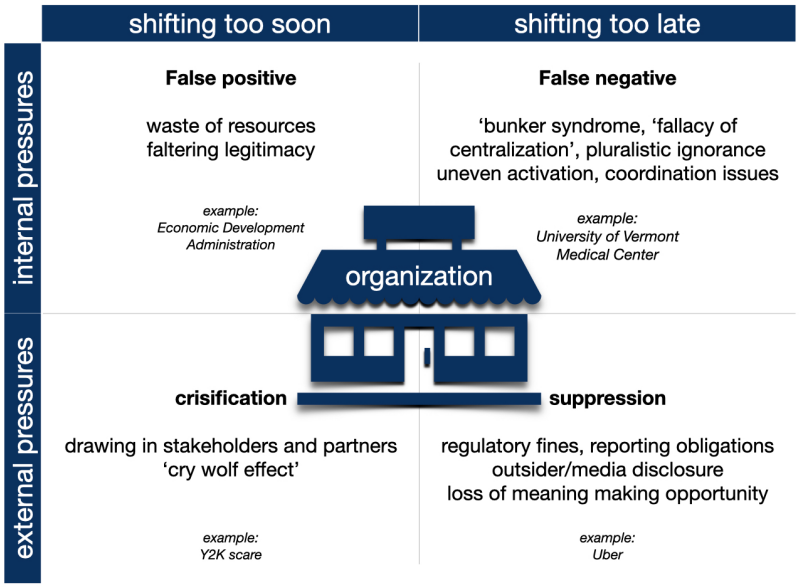


**Figure 1. Typology: internal and external pressures when switching from cyber incident to crisis management**

### Internal pressure 1 – False positive: calling a crisis too soon

SOCs process vast numbers of alerts daily, and the problem of false positives in a high-noise environment is widely documented as a central operational challenge (Tariq et al., 2025). When analysts overestimate the severity of an alert during triage, under conditions of time pressure, uncertainty, and alert fatigue, organizations may escalate incidents prematurely. Such early escalation can result in misallocated resources, unnecessary disruption, and reduced attention to genuinely critical events. Prior research shows that SOCs frequently struggle to distinguish between benign anomalies and true indicators of compromise, especially when user behavior or legitimate research activities mimic malicious patterns (Sundaramurthy et al., 2014).

Further, technical unfamiliarity or inexperience may exacerbate this. A prominent example of premature escalation occurred at the U.S. Economic Development Administration in 2011. A common malware infection of a small number of computers, remediable through routine technical actions, was misinterpreted as a systemwide compromise, due to internal miscommunication and analyst inexperience. As a result, the agency spent almost half of its yearly IT budget, close to 3 million dollars, on response efforts including destroying and renewing hardware, hiring cybersecurity contractors, remaining with impaired systems for almost an entire year (Rein, 2013). This case illustrates how misjudgments during incident assessment can quickly propel an organization into unnecessary crisis-mode responses.

Internal organizational dynamics can reinforce tendencies toward early escalation. Crisis scholarship warns that organizations may activate crisis structures prematurely when sensemaking processes are distorted by uncertainty, miscommunication, or institutional pressures (Pearson and Mitroff, 1993; Boin et al., 2017). However, repeated unnecessary escalation risks eroding organizational credibility, diminishing trust in incident response assessments, and weakening support for activating crisis management structures when escalation is needed.

### Internal pressure 2 – False negative

Missing or narrowly interpreting warning signals of an escalating incident can delay or derail a timely response. This is known as the false negative. When early indications of system compromise are not integrated into a common operational picture, coordination may falter in the initial stages. Crises can be sensed at different moments within an organization, and not necessarily by those with formal authority to declare escalation. In control-room and SOC environments, frontline operators are often first to observe anomalies or emerging patterns of concern, while the translation of these signals into organization-wide action may occur only much later (Tøndel et al., 2014). This temporal disconnect increases the risk that organizational leadership responds only after the situation has deteriorated. Recognizing false negatives in a digital environment is challenging, due to constantly evolving attack patterns, attackers using sophisticated evasion techniques, and the challenge of detecting

anomalies across large, complex network traffic. Cybersecurity contexts may also differ from fast-response and high-reliability organizations where preoccupation with failure is an established principle, in that impression management can inhibit incident escalation. As Dalal et al. (2016) note, SOC analysts may hesitate to escalate due to fear of negative judgment rather than being encouraged to treat mistakes as part of the process.

Crisis scholarship highlights how different socio-cognitive dynamics can impede accurate sensemaking during a crisis. Boin et al. (2017) warn for a so-called 'bunker syndrome', describing the tendency of members to stick together and reify their own view of the crisis in relative isolation (p. 47). Similarly, the 'fallacy of centralization' may emerge when a team believes that their central position guarantees full situational awareness, and a lack of incoming updates means nothing significant is occurring (Boin et al. 2017). Likewise, Weick (1990) points to the risk of 'pluralistic ignorance', when individuals assume that others will take necessary action and see little need to intervene themselves. Taken together, these socio-cognitive dynamics illustrate a range of constraints that undermine sensitivity to operational signals.

These sensemaking challenges are compounded when organizations lack a common operational picture that spans units, disciplines, or layers of hierarchy (Wolbers and Boersma, 2013). During cyber incidents, different teams may adapt to emerging disruptions unevenly, implement quick fixes of uncertain effectiveness, or enact in deviating response strategies. Without mechanisms for integrating incongruent actions, the organization's response is likely to become disconnected, or even contradictory (Ahmad et al., 2020; Wolbers & Schakel, 2021). Such responses contribute directly to delays in recognizing the incident as a crisis and mobilizing the appropriate response structures.

Such dynamics are visible in the cyberattack at the University of Vermont Medical Center in 2020, which led to 25 days of operational downtime (Stowman & Kalof, 2022). On the day of the attack, clinical units and operating rooms shifted to paper-based operations, while the anatomic pathology laboratory followed its established protocols and ceased operations entirely. As many hospital departments remained functional and continued to treat patients, the laboratory shutdown gradually became a bottleneck for the entire organization. The delay in recognizing the system-wide consequences of deviating local incident management strategies contributed to prolonged disruption. Only after the laboratory implemented an internal incident command system to reorganize workflows did operations stabilize, illustrating how delayed escalation and the absence of shared situational awareness can amplify the impact of a cyber incident.

#### External pressure 3 – Crisification

Organizations may also face external pressures when escalation is premature. When an incident is publicly framed as a crisis too soon, it may unnecessarily activate the broader network of stakeholders, such as regulators, partner organizations, service providers, and public authorities, who hold a vested interest in crisis response. Mobilizing these actors prematurely can strain interorganizational relationships, divert scarce resources, and generate reputational concerns if the situation later appears overblown. Moreover, escalating too early can provoke anxiety among clients, customers, or citizens who rely on the organization's services. In sectors such as healthcare, finance, or public administration, early crisis declarations may be interpreted as indicators of systemic vulnerability, thereby amplifying fear or uncertainty in ways disproportionate to the actual incident (Bhatt et al., 2025). Specifically, in cybersecurity, the public's understanding of the consequences may also be less advanced in comparison to crises in other domains.

In crisis management literature, this phenomenon is discussed as the 'cry wolf' syndrome, where premature crisis declarations erode the credibility of organizational signals over time (Lim et al., 2019). When stakeholders perceive that crisis labels are applied too readily, organizational legitimacy may suffer, reducing the likelihood that future warnings are taken seriously (Pearson and Mitroff, 1993). This is particularly relevant in cybersecurity, where the boundary between an incident and a crisis is often ambiguous. Such uncertainty may create incentives for organizations to escalate defensively to demonstrate vigilance to regulators or the public (Backman, 2021).

Security studies scholarship provides additional conceptual tools to understand these pressures. Securitization highlights how framing an issue as a security threat enables extraordinary measures and resource mobilization but also requires the actor making the claim to maintain credibility with its audience (Gomez & Whyte, 2021). Over-securitizing routine incidents risk 'crisification', the overextension of crisis language and structures to situations that do not warrant them. This aligns with longstanding concerns in crisis scholarship about expanding crisis discourse to routine disruptions, thereby undermining the distinctiveness and effectiveness of crisis governance (Rosenthal et al., 1989). An example of this relates to the Y2K scare, the global panic regarding the built-in clocks of computers in the late 1990s. These clocks oftentimes used 2 digit-dates, which led to the fear that these computers would crash at the turn of the Millenium, because their clocks would revert to 1 January 1900 instead of 1 January 2000. Multi-billion investments were made by companies worldwide to remedy this flaw. In hindsight

experts have expressed doubts about the proportionality and even the necessity of that response.

### External pressure 4 – Suppression

Organizations may also face external pressures that inadvertently delay escalation to crisis mode. Under regulatory regimes such as the European Union's NIS2 directive organizations have mandatory reporting obligations for significant cyber incidents. Failure to report within prescribed timelines can lead to substantial fines and increased scrutiny from supervisory authorities. Paradoxically, this regulatory pressure may create incentives for organizations to downplay incidents during early stages, delaying escalation until they have gathered sufficient information to meet reporting thresholds, or avoid misclassifying routine events as significant incidents. Studies of incident response structures suggest that organizations often try to 'contain' events internally before activating external disclosure processes, both to align with regulatory requirements and to protect organizational reputation (Ahmad et al., 2012; Onwubiko & Ouazzane, 2020).

External discovery of an incident represents an additional pressure point that can complicate escalation timing. If a breach becomes public through third parties like affected users, suppliers, or the media, the organization may lose its ability to frame and interpret the incident for its stakeholders. External discovery is a risk in data extortion cases, where the attacker may pivot to publishing the data in a leak blog, or to contacting the individual victims directly (Ghanbari & Koskinen, 2024).

Notably, organizations do not have the sole authority to call out a crisis. This is often illustrated by an amended version of the Thomas Theorem: '*if people define a situation as a crisis, it is a crisis in its consequences'*. Crisis communication scholarship repeatedly emphasizes that when organizations lose their meaning making opportunity, they also lose control over how the event is framed (Kuipers & Wolbers, 2021). Regardless of the organization's own assessment, it is compelled to respond at crisis scale, often from a position of disadvantage.

During its 2016 data breach, Uber initially attempted suppression. In October of that year hackers stole data of over 57 million Uber users and drivers. To suppress the crisis, Uber management decided to pay off the attackers if they promised to delete the data. When new management took over in 2017, they discovered the hack and its attempted resolution and reported it to the media. Uber's attempt to mitigate the crisis was widely condemned, gave rise to regulatory investigations, and led to various lawsuits (McGovern, 2024). Uber's suppression of the breach allowed external narratives to fill the void, accelerating the crisis from the outside rather than from within.

## CONCLUSION

Understanding when a cyber incident becomes a cyber crisis requires more than technical severity metrics. It demands attention to organizational cognition, coordination, and insight into the audiences that construct a crisis status. Both over- and under-escalation carry material and reputational costs, especially when meaning making is taken over by third parties. Practically, organizations can codify crisis thresholds, institutionalize common operational pictures, and align incident response with governance and strategic communication.

In this paper, we foreground a preliminary typology on how internal and external pressures, early and late responses, may shape the timing, legitimacy, and effectiveness of different responses. The typology may provide a starting point for studies into when and how cyber incidents escalate into cyber crises. Next steps include an exploration and validation of the typology across institutional and operational contexts, to distill considerations specific to cyberspace as a crisis medium. Conceptually, we invite empirical testing of the typology across sectors and regulatory contexts.

## REFERENCES

Ahmad, A., Hadgkiss, J., & Ruighaver, A. B. (2012). Incident response teams. Challenges in supporting the organizational security function. *Computers & Security*, *31*(5), 643-652. https://doi.org/10.1016/j.cose.2012.04.001

Ahmad, A., Desouza, K. C., Maynard, S. B., Naseer, H., & Baskerville, R. L. (2020). How integration of cyber security management and incident response enables organizational learning. *Journal of the Association for Information Science and Technology*, *71*(8), 939-953. https://doi.org/10.1002/asi.24311

Backman, S. (2021). Conceptualizing cyber crises. *Journal of Contingencies and Crisis Management*, *29*(4), 429-438. https://doi.org/10.1111/1468-5973.12347

Berg, B. van den, & Kuipers, S. L. (2022). Vulnerabilities and cyberspace: a new kind of crisis. *Oxford Research Encyclopedia of Politics.* https://doi.org/10.1093/acrefore/9780190228637.013.1604

Bhatt, P., Valecha, R., & Rao, H. R. (2025). Situational awareness about data breaches and ransomware attacks: A multi-dimensional cyber threat impact framework and content analyses of practitioner-public discourses. *International Journal of Information Management*, *83*, 102902. https://doi.org/10.1016/j.ijinfomgt.2025.102902

Boin, A., Hart, P. T., & Kuipers, S. (2017). *The Crisis Approach*. In Handbook of Disaster Research (pp. 23-38). Cham: Springer International Publishing. https://scholarlypublications.universiteitleiden.nl/handle/1887/62805

Brown, J. M., Greenspan, S., & Biddle, R. (2016). Incident response teams in IT operations centers: the T-TOCs model of team functionality. *Cognition, Technology & Work*, *18*(4), 695-716. https://doi.org/10.1007/s10111-016-0374-2

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer security incident handling guide. *NIST Special Publication*, *800*(61), 1-147.

Lee, M., Mercer, W., Rascagneres P., & Williams, C. (2017, May 12). Player 3 Has Entered the Game: Say Hello to 'WannaCry'. Cisco Talos https://blog.talosintelligence.com/wannacry/

Dalal, R.S., Bolunmez, B., Tomassetti, A, J., & Sheng, Z. (2016). Escalation. An Understudied Team Decision-Making Structure. In S.J. Zaccaro, R.S. Dalal, L.E. Tetrick & J.A. Steinke (Eds), *Psychosocial Dynamics of Cyber Security.* (pp. 18-35). Routledge. https://doi.org/10.4324/9781315796352

DeNardis, L. (2020). *The Internet in Everything: Freedom and Security in a World with No off Switch*. Yale University Press.

Department of Homeland Security (2023). *Harmonization of Cyber Incident Reporting to the Federal Government*. https://www.dhs.gov/sites/default/files/2023-09/Harmonization%20of%20Cyber%20Incident%20Reporting%20to%20the%20Federal%20Government.pdf.

ENISA. (2024). *Best Practices for Cyber Crisis Management.* https://www.enisa.europa.eu/publications/best-practices-for-cyber-crisis-management

Ghanbari, H. & Koskinen, K. (2024). When data breach hits a psychotherapy clinic: The Vastaamo case. *Journal of Information Technology Teaching Cases, 1-9.* https://doi.org/10.1177/20438869241258235

Gomez, M. A., & Whyte, C. (2021). Breaking the myth of cyber doom: Securitization and normalization of novel threats. *International Studies Quarterly*, *65*(4), 1137-1150. https://doi.org/10.1093/isq/sqab034

He, Y., Zamani, E. D., Lloyd, S., & Luo, C. (2022). Agile incident response (AIR): Improving the incident response process in healthcare. *International Journal of Information Management*, *62*, 102435. https://doi.org/10.1016/j.ijinfomgt.2021.102435

Kaspersky (2017). New Petya / NotPetya / ExPetr ransomware outbreak. https://www..com/blog/new-ransomware-epidemics/17314/

Kuipers, S., & Wolbers, J. (2021). Organizational and institutional crisis management. In *Oxford Research Encyclopedia of Politics*. https://doi.org/10.1093/acrefore/9780190228637.013.1611

Kuipers, S., Perlstein, S., Wolbers, J., & Jong, W. (2023). Assist or accuse? Identifying trends in crisis communication through a bibliometric literature review. *Risk, Hazards & Crisis in Public Policy*, *14*(4), 272-296. https://doi.org/10.1002/rhc3.12283

Lakshmi, R., Naseer, H., Maynard, S., & Ahmad, A. (2021). Sensemaking in cybersecurity incident response: The interplay of organizations, technology and individuals. https://doi.org/10.48550/arXiv.2107.02941

Lim, J. R., Liu, B. F., & Egnoto, M. (2019). Cry wolf effect? Evaluating the impact of false alarms on public responses to tornado alerts in the southeastern United States. *Weather, Climate, and Society*, *11*(3), 549-563. https://doi.org/10.1175/WCAS-D-18-0080.1

Madani, A., Rezayi, S. & H. Gharaee (2011). Log Management comprehensive architecture in Security Operation Center (SOC), *2011 International Conference on Computational Aspects of Social Networks (CASoN).* doi**:** 10.1109/CASON.2011.6085959

McGovern, V. (2024). *Uber: Cyber breaches*. SAGE Publications: SAGE Business Cases Originals.

Mugu, S. R., Zhang, B., Kolla, H., Balaji, S. R. A., & Ranganathan, P. (2024). Lessons from the CrowdStrike incident: assessing endpoint security vulnerabilities and implications. In *2024 Cyber Awareness and Research Symposium (CARS)* (pp. 1-10). IEEE.

Nelson, A., Rekhi, S., Souppaya, M., & K. Scarfone (2025). *Incident Response Recommendations and Considerations for Cybersecurity Risk Management*, National Institute of Standards and Technology, U.S.

Department of Commerce. https://doi.org/10.6028/NIST.SP.800-61r3

Onwubiko, C., & Ouazzane, K. (2020). SOTER: A playbook for cybersecurity incident management. *IEEE Transactions on Engineering Management*, *69*(6), 3771-3791. doi**:** 10.1109/TEM.2020.2979832

Pearson, C. M., & Clair, J.A (1998) Reframing Crisis Management. *Academy of Management Review, 23*(1), 59-76. https://www.jstor.org/stable/259099

Pearson, C. M., & Mitroff, I. I. (1993). From crisis prone to crisis prepared: A framework for crisis management. *Academy of Management Perspectives*, *7*(1), 48-59. https://www.jstor.org/stable/4165107

Phillips, R., & Tanner, B. (2019). Breaking down silos between business continuity and cyber security. *Journal of Business Continuity & Emergency Planning*, *12*(3), 224-232. https://EconPapers.repec.org/RePEc:aza:jbcep0:y:2019:v:12:i:3:p:224-232

Prevezianou, M. F. (2021). Beyond ones and zeros: Conceptualizing cyber crises. *Risk, Hazards & Crisis in Public Policy*, *12*(1), 51-72. https://doi.org/10.1002/rhc3.12204

Rein, L. (2013, July 14). *At Commerce Dept., false alarm on cyber-attack cost almost $3 million*. Washington Post. https://www.washingtonpost.com/politics/at-commerce-dept-false-alarm-on-cyberattack-cost-almost-3-million/2013/07/13/11b92690-ea41-11e2-aa9f-c03a72e2d342_story.html

Rosenthal, U., Charles, M., & 't Hart, P. (Eds.) (1989). *Coping with crises: The management of disasters, riots and terrorism.* Charles C. Thomas. https://doi.org/10.2307/2393212

Roux-Dufort, C. (2007). Is crisis management (only) a management of exceptions? *Journal of Contingencies and Crisis Management*, *15*(2), 105-114. https://doi.org/10.1111/j.1468-5973.2007.00507.x

Ruohonen, J., Rindell, K., & Busetti, S. (2025). From cyber security incident management to cyber security crisis management in the European Union. *Computers & Security*, 104689. https://doi.org/10.1016/j.cose.2025.104689

Schakel, J. K., van Fenema, P. C., & Faraj, S. (2016). Shots fired! Switching between practices in police work. *Organization Science*, *27*(2), 391-410. https://www.jstor.org/stable/24763309

Schakel, J. K., & Wolbers, J. (2021). To the edge and beyond: How fast-response organizations adapt in rapidly changing crisis situations. *Human Relations*, *74*(3), 405-436. https://doi.org/10.1177/0018726719893450

Stowman, A. M., & Kalof, A. N. (2022). Surviving a Cyberattack in Anatomic Pathology: Disaster Response and Creation of an Incident Command System. *American Journal of Clinical Pathology: Reviews & Reports*, *27*(4), 171-176. 10.1097/pcr.0000000000000519

Sundaramurthy, S. C., Case, J., Truong, T., Zomlot, L., & Hoffmann, M. (2014). A tale of three security operation centers. In *Proceedings of the 2014 ACM workshop on security information workers* (pp. 43-50). https://doi.org/10.1145/2663887.2663904

Tariq, S., Baruwal Chhetri, M., Nepal, S., & Paris, C. (2025). Alert fatigue in security operations centres: Research challenges and opportunities. *ACM Computing Surveys*, *57*(9), 1-38. https://doi.org/10.1145/3723158

Tøndel, I. A., Line, M. B., & Jaatun, M. G. (2014). Information security incident management: Current practice as reported in the literature. *Computers & Security*, *45*, 42-57. https://doi.org/10.1016/j.cose.2014.05.003

Turner, B. A. (1976). The organizational and interorganizational development of disasters. *Administrative Science Quarterly*, 378-397. https://www.jstor.org/stable/2391850

Vielberth, M., Böhm, F., Fichtinger, I., & Pernul, G. (2020). Security operations center: A systematic study and open challenges. *IEEE Access*, *8*, 227756-227779. doi**:** 10.1109/ACCESS.2020.3045514

Wired (2018, August 22). The Untold Story of NotPetya, the Most Devastating Cyberattack in History.https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Weick, K. E. (1990). The vulnerable system: An analysis of the Tenerife air disaster. *Journal of Management*, *16*(3), 571-593. https://doi.org/10.1177/014920639001600304

Wolbers, J., & Boersma, K. (2013). The common operational picture as collective sensemaking. *Journal of Contingencies and Crisis Management*, *21*(4), 186-199. https://doi.org/10.1111/1468-5973.12027

Wolbers, J. (2022). Understanding distributed sensemaking in crisis management: The case of the Utrecht terrorist attack. Journal of Contingencies and Crisis Management, 30(4), 401-411. https://doi.org/10.1111/1468-5973.12382

Wolbers, J., van Steen, T., Del-Real, C., & van den Berg, B. (2025). Cyber crisis averted: using safety science principles to learn from success. In Proceedings of the International ISCRAM Conference. https://doi.org/10.59297/sfxddg82