# Managing Ambiguity in Crisis Escalation Procedures

Published 30 January 2020 - ID G00717462 - 13 min read

Enterprise Risk Management Research Team

Initiatives:Risk Response Strategies **and 5 more**

Crisis escalation procedures are often ambiguous, resulting in delays in getting critical information to those responsible for the crisis management plan, which leads to slower response times. This research provides heads of enterprise risk management solutions to this challenge.

## Overview

The earliest moments of a crisis heavily influence the enterprise's crisis management effectiveness. Waiting too long to communicate risk event information and escalate action can hamper the organization's ability to effectively respond to an issue and mitigate major losses. While organizations often have standardized policies and procedures designed to guide employees through a crisis, many struggle to operationalize these escalation procedures due to the ambiguity inherent in the business's decision to escalate during a risk event.

To navigate this ambiguity in determining risk escalation triggers, heads of enterprise risk management involved in crisis management should transition from scenario-based planning to impact-based planning, create a simple matrix to guide quick escalation decisions and conduct a postmortem after crisis events to provide better guidelines for future issues.

### Key Findings

- Using a scenario-based approach to create crisis escalation procedures results in uncertainty because it can't create precise scenarios that accurately predict how events will manifest. Instead, ERM should take an impact-based approach to plan around critical systems and processes that are affected by crises that develop regardless of the specifics of a given risk event.
- Providing the business leader who is responsible for escalating issues to the crisis management team with a simple, one page matrix offers quick guidance for when escalation is appropriate during consequential crisis events.
- Conducting postmortem exercises following crises can highlight areas of improvement, reducing ambiguity in future situations of how and when to escalate risk information.

### Introduction

When the malware NotPetya first hit in 2017, shipping giant Maersk was unable to determine exactly what was occurring. According to news accounts at the time, it took several hours to establish the cause of the attack and subsequent widespread impact. The attack affected IT services, end-user devices, and applications and servers. As many as 49,000 laptops were destroyed and 1,200 applications were locked up.

Once the issue was identified, Maersk moved quickly, working with trusted external specialists on cyber forensics. The company designed a new Windows build, retrieved an undamaged copy of the active directory and rebuilt it, strengthened its firewall and was as transparent as possible about the incident, both internally and externally. Maersk even spoke with the individual responsible for creating the NotPetya malware.

Though Maersk suffered losses of over $250 million, its quick response to the crisis ensured its continuity. According to Maersk's head of technology, 95% of goods being transported by shipping containers during the crisis arrived at their destination on time. Moreover, Maersk remains the largest container shipping company in the world. This illustrates the importance of expedient responses to crisis events.

Speedy and prescient action in response to a crisis could determine the fate of a company, as evidenced by Nokia and Ericsson's response to the same crisis. A fire broke out at a Royal Philips Electronics mobile phone microchip plant in Albuquerque, New Mexico in March 2000. This crisis altered the fates of the two rival telecommunications companies. According to news accounts, employees at the plant discovered smoke from the fire and water from the sprinklers had contaminated and destroyed millions of microchips awaiting shipment. Most notably, two titans of the mobile phone industry, Nokia and Ericsson, were waiting for these shipments.

The extent of the damage from this event was not initially clear. Philips at first assured the companies it would be able to make a quick fix, causing disruptions for only a week. Nevertheless, Nokia moved quickly in response to the event, working with Philips' executive management to free up capacity at alternative factories. At the same time, a team of engineers redesigned some phones to accommodate chips from other Philips and non-Philips plants. Another group worked to find new manufacturers to reduce the burden on Philips.

While Nokia acted swiftly in response to the crisis, Ericsson adopted a "wait and see" approach instead of developing contingency plans. Two weeks after the fire, Philips reported the incident was more severe than previously stated. By then, it was too late for Ericsson to effectively manage the crisis. The Philips plant ultimately was shut down for six weeks. Ericsson reported second quarter operating losses in its mobile phone division of $200 million and never recovered, ceding market share to Nokia and eventually merging with Sony Corporation to survive. Meanwhile, Nokia emerged from the crisis even stronger, reporting a 30% increase in global market share by the end of the third quarter in 2000.

This example highlights the difficulty and importance of the decision to trigger crisis management plans. It was not originally clear if this microchip shortage would indeed be a crisis. It was only a

couple of weeks after the fire that the severity of the disruption became clear. However, because Nokia dealt with this ambiguity better than Ericsson, it was able to stem the losses and gain a competitive advantage over its competitor. While navigating the ambiguity inherent in triggering crisis management plans is difficult, doing it effectively is vital to ensure a company's well-being.

At the heart of this challenge is the difficult and high-stakes decision to trigger a crisis management plan. Trigger it prematurely and you risk wasting resources and being seen as the "boy who cried wolf." Trigger the plan too late and the organization can suffer severe financial, reputational and legal consequences. Employees are often caught between making a choice to escalate risk event information or relying on regular processes to solve the problem, which could fall short or make matters worse. Fortunately, ERM teams can take concrete steps to ensure they effectively manage this ambiguity.

### Implement Impact-Based Crisis Escalation Planning

When creating crisis-escalation procedures, ERM will often attempt to plan for specific scenarios of a given risk event. ERM teams believe they must account for all possible variables affecting a risk event to make escalation plans as precise as possible, enabling effective escalation guidance for specific crisis scenarios. Unfortunately, this often leads to more ambiguity and less effective crisis management because precisely predicting the multitude of ways a risk event could play out is impossible.

A risk event will always develop differently than what is planned, leading to delayed escalation while the business is forced to go off-script. Because time is of the essence during a crisis, any delay in escalation can severely hamper mitigation and recovery efforts. Instead of constructing crisis management escalation procedures to deal with specific scenarios, ERM should build its procedures around critical enterprise-level impacts regardless of the specifics of the risk event. Once risk-event information is escalated, the team responsible for managing the crisis will initiate its predefined plan for the impacted areas, including response and recovery steps, communication procedures and people management. The team will also tailor the plan for the specific variables at play.

Critical impacts from crises are typically the same regardless of the risk event. For instance, while fires, floods and earthquakes are distinct scenarios, the critical impacts the business is concerned with are the same: systems outage, employee absence, supply chain disruption, etc. Scenario planning for each type of natural disaster would be resource-intensive and challenging due to all the unknowns. Planning for a systems outage, for example, regardless of the cause, takes less effort as it covers multiple crisis events. This reduces ambiguity as employees are not left scrambling when an event does not develop as planned. Rather, employees can escalate risk event information when certain critical systems and processes are significantly impacted by an event. To operationalize escalation procedures, ERM can create a simple matrix highlighting appropriate escalation actions for critical impacts.

### Simplify Escalation Guidance

Organizations use complicated flowcharts or in-depth policy manuals to guide escalation decisions during times of crisis. These can be difficult to decipher and time-consuming to follow, resulting in slower responses as the employees struggle to decide whether to escalate risk event information. Instead, ERM should provide simple escalation guidance that can facilitate quick decision making.

**Case in Point: GrayHarbor's* Escalation Thresholds and Criteria Guidelines**

GrayHarbor's ERM team was concerned its business resiliency managers — the parties responsible for escalating risk event information — would be delayed in their decision making by providing overly specific guidance that failed to be applicable as an actual crisis event unfolded.

To fix this, ERM created a simple matrix to guide focused and appropriate response. ERM first identified three event categories (by order of magnitude) with instructions on how to escalate and to whom:

- **Incident** — An incident is typically an emergency that can be effectively handled within the parameters of established emergency response and incident management plans of a particular business unit, function or location. The incident is not likely to escalate to an issue or crisis and therefore, does not need to engage the crisis response team (CRT). The global business resilience (GBR) team is notified through routine incident reporting mechanisms, usually after the incident has been resolved.

- **Issue** — An issue is typically a regional or significant cross-functional emergency incident requiring management beyond a single team or activation of a business continuity plan. Although an issue will have the potential to damage the company's reputation and/or have serious regulatory consequences locally or within a specific business unit, an issue would not seriously threaten the company's global reputation or assets. GBR is alerted via telephone and the issue may be managed or simply supported by the CRT.

- **Crisis** — A crisis has the potential to cause serious damage to the company and as such must be managed by the crisis management team (CMT). A crisis may be determined at the outset or as a result of an escalating event or incident. GBR must be notified immediately by telephone and will activate the CMT.

ERM then created a matrix to establish trigger points for each major impact category (see Table 1).

The business resiliency manager is instructed to escalate once a single criteria crosses a threshold. For instance, if the business resiliency manager assesses operational impact as growing from a single region to multiple regions, they should follow the crisis escalation

protocols and immediately notify the GBR team, who will activate the crisis management plan. This method helps provide the business with actionable escalation guidance while avoiding the trap of being overly specific and gives the business resiliency manager the freedom to use their judgment when assessing risk events.

*Pseudonym.

Table 1: Escalation Criteria Matrix

| Category | Incident | Issue | Crisis |
|---|---|---|---|
| Financial Impact | Potential financial losses are likely to be less than $X million. | Potential financial losses are likely to be greater than $X million but less than $YY million. | Potential financial losses are likely to be greater than $YY million. |
| Operational Impact | ■ Local impact — e.g., single location or system.<br>■ Impact is limited to one asset or site only. | ■ Regional/business impact.<br>■ More than one asset, location or a major asset, location and/or several business functions impacted.<br>■ Effects are limited to one region but actual or potential for expanding effects nationally. | ■ Corporatewide impact.<br>■ Multiple major assets, locations and/or business functions affected or potentially affected. |

| | | | |
|---|---|---|---|
| Technology Impact | ■ System/application outage impacting a single business unit/location.<br>■ Routine IT incident management processes. | ■ System/application outage affecting multiple business units (e.g., an enterprise application).<br>■ Cybersecurity incident that is causing business impact.<br>■ Customer communications required to be sent out by more than one business unit. | ■ Data center down, inaccessible or multiple enterprise systems otherwise unavailable; immediate notification required.<br>■ Escalation of an issue category event due to an expected outage duration of longer than four hours.<br>■ Total loss of a data center. |
| Traditional Media/Social Media Coverage | ■ Unlikely to be of interest outside of the local market. No company brand impact.<br>■ No corporate statement required or routine/not time-sensitive statement developed as a normal course of business. | ■ Actual or potential interest, which is unlikely to significantly damage company brand but urgent corporate response may be necessary. | ■ Media coverage is likely to cause significant damage to company brand impact.<br>■ Immediate corporate response is required. |
| People Impact | ■ Internal: Associate(s) are affected, but implications are minimal.<br>■ External: Customer(s) and patient(s) are affected, but implications are minimal. | ■ Internal: Associate(s) are affected, but implications are moderate.<br>■ External: Customer(s) and patient(s) are affected, but implications are moderate. | ■ Internal: Associate(s) are affected, and implications are significant.<br>■ External: Customer(s), patient(s) and/or community(s) are affected, and implications are significant (magnitude and/or duration of impact). |

| | | | |
|---|---|---|---|
| Health and Safety Impact | Injury and/or illness resulting in first aid or first responder treatment. | Injury and/or illness resulting in emergency medical treatment or non-work-related loss of life in the workplace. | Injury and/or illness resulting in advanced medical treatment or loss of life. |
| Regulator Impact | No or routine regulator(s) interest. | Inquiry-level interest from a regulator(s); considered a reportable incident and/or a potential action against a license. | Regulator(s)-targeted interest in the situation, and/or demanding action(s) by company, and/or an immediate unplanned action against a license. |
| Share Price Sensitivity | No or anticipated share price sensitivity. | Unanticipated moderate negative share price sensitivity. | Unanticipated significant negative share price sensitivity. |

Source: GrayHarbor*

Once a crisis has been contained and the business has returned to normal operating procedures, organizations must assess the effectiveness of their escalation procedures. This provides lessons about what went well and what needs to be improved for future crises. To facilitate this, ERM should conduct a postmortem.

### Crisis Escalation Postmortem

During the restoration process following a crisis, ERM must debrief the event with the major stakeholders involved to assess response effectiveness. Evaluating the process in a group setting enables cross-functional feedback, allowing ERM to understand how each stakeholder's decisions affected the other stakeholders during the crisis. For instance, a delay in escalation from a business unit leader to the CMT can significantly delay crisis management plan activation, leading to major disruptions throughout multiple functions.

For the business, this highlights the importance of timely escalation by demonstrating the consequences of delayed action. Moreover, this shines a spotlight on the delay, allowing ERM to dig deeper and develop an action plan to ensure subsequent crises are escalated to the CMT quicker, saving the company from future lost revenue, reputational damage and perhaps even loss of life. ERM will then update its crisis escalation plans and disseminate them to the business to reflect on lessons learned from the postmortem.

## Conclusion

The decision to escalate risk event information is critical to ensure effective crisis management. Costly delays occur when escalation guidance is ambiguous, leading to employee uncertainty

about when and how to escalate risk event information. Fortunately, ERM can take several steps to make these decisions less ambiguous.

Transitioning from a scenario-based crisis management approach to an impact-based approach simplifies escalation decisions as employees have greater certainty about what to do — even when a crisis plays out differently than planned. An impact-based approach that focuses escalation guidance on critical impacts provides clarity because impacts are generally the same regardless of crisis event, reducing the number of variables an employee must weigh when considering escalation.

ERM should also provide employees who are responsible for escalation with a simple matrix that highlights appropriate escalation actions for critical impacts. Compared to traditional flowcharts and policy manuals, this approach expedites escalation decisions by providing employees with only the most crucial information relevant for their role in crisis escalation. Lastly, ERM must conduct a postmortem with key stakeholders following a crisis. This allows ERM to identify points in the escalation process that can be improved in future crises. With these approaches, ERM can ensure more effective crisis management.

## Recommended by the Authors

- "Crisis Management: Closing the Loop (Intuit)" — Intuit's ERM team created a closed loop crisis management process to effectively manage crisis and enhance ongoing response plans. Heads of ERM can use this approach to ensure timely response to information security crisis incidents and reduce the organization's risk exposure.
- "Crisis Communication Plan Templates" — Use these sample crisis communication plans for different business functions to help inform, create and update your own.
- "Crisis Communications Plan Builder" — This tool will help you create your own customized crisis communication plan that captures the critical elements for managing crises.
- "Crisis Readiness Assessment Tool" — These tools will help you assess your organization's readiness and preparedness to address crises.

## About This Research

This study is based on multiple interviews with heads of ERM and their teams, as well as original Gartner research.

## Recommended For You

Crisis Management: Closing the Loop (Intuit)

Amplifier Risks (GraySpring*)

Ignition Guide to Managing Emerging Risks