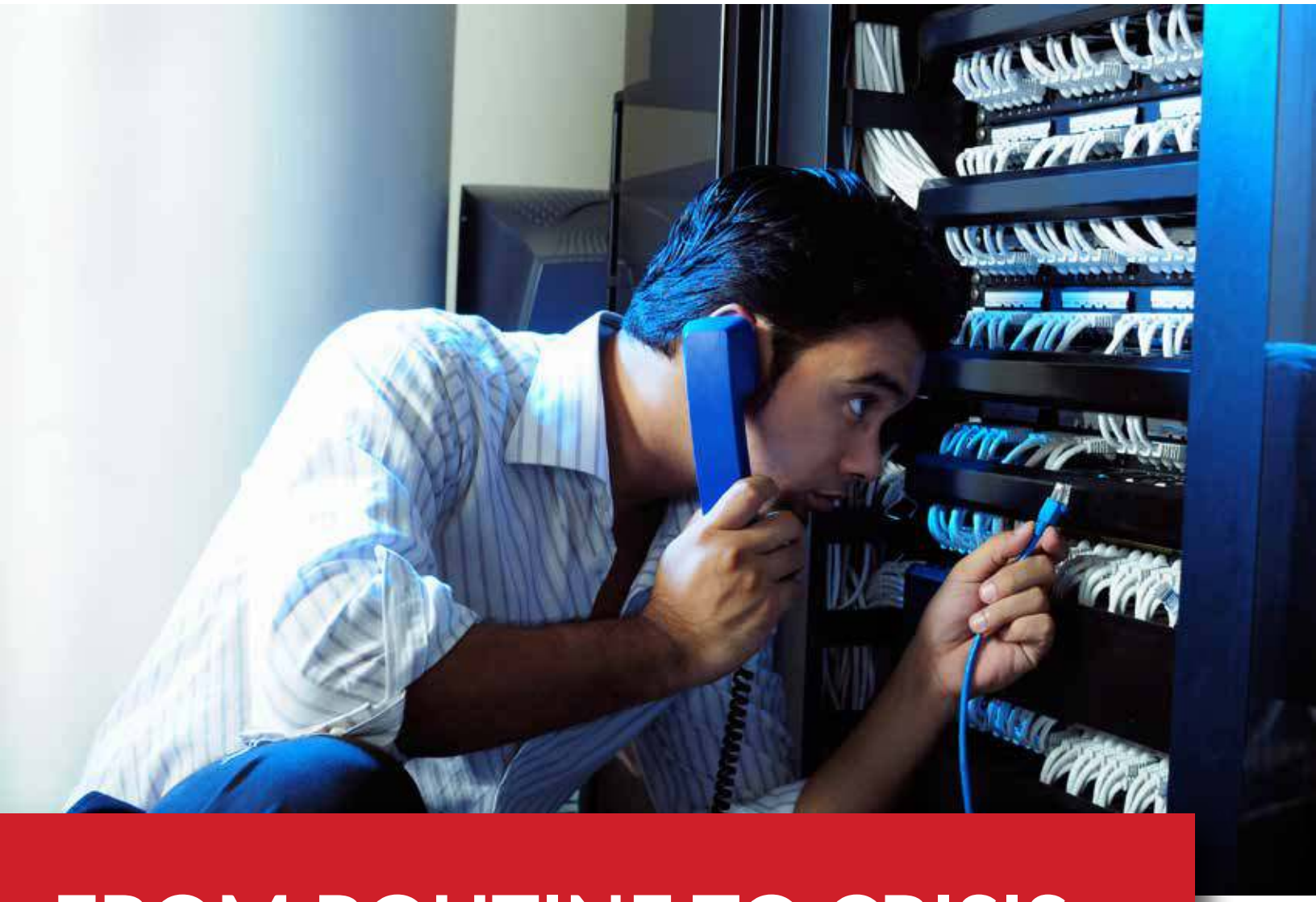
everbridge®



FROM ROUTINE TO CRISIS: HANDLING AN ESCALATING IT INCIDENT

by – **Regina Phelps, CEM, RN, BSN, MPA** and **Kelly David Williams**

WWW.EVERBRIDGE.COM

From Routine to Crisis: Handling an Escalating IT Incident

By Regina Phelps and Kelly David Williams

Introduction

Emergencies happen frequently in the world of technology. There are equipment failures, network snafus, and application meltdowns. Technology professionals are quite used to – and very adept at – being in the "fire-fighting" role. But what happens when the basic, old, "run-of-the-mill" emergency turns into a full-blown corporate-wide crisis?

Questions that deserve careful thought include:

- ✓ When an incident occurs, who evaluates the potential impact, and how do they do that?
- ✓ Does the impact assessment mechanism take business ramifications into full account?
- ✓ Based on the potential impacts, who should be notified and how quickly?
- ✓ Does the escalation procedures include relevant business partners, in addition to IT resources and management?
- ✓ What communications channels/tools do you use for notifications and ongoing coordination? Are they adequate for the purpose in a large-scale, rapidly evolving incident?

Limited or Crisis?

Although there are many types of incidents, I am placing them all into two general categories. The first is limited impact. It can be difficult and it can be onerous, however, it is just that – limited.

For this paper, the incident I want to discuss is the crisis incident – a technology problem with far-reaching impact. It impacts the user (both internal and external), production, and productivity, and/or it can impact the company brand or reputation. The big difference between the two types of incidents is the IMPACT of the incident.

"Give Me Five Minutes"

I often tease IT professionals about this phrase, often heard in the technology halls during an incident. "Please just give me five more minutes!" This implies if they just had a few more minutes they would certainly solve the problem. "Don't escalate this; I almost have it!"

What this approach fails to take into account, however, is the impact that is likely occurring *outside* those technology halls. While the IT professionals are working diligently to fix the problem, many users are feeling the impact. While the technician is diligently working on the solution they will have in "just five minutes," production, productivity, and a blow to brand/reputation are happening. The solution to this is to ensure that your assessment and communications reach those who need to be part of the assessment and communication. In other words, you must have a quick escalation procedure, and timely communication strategy.

Impact!

Getting your arms around the somewhat nebulous concept of impact can be like a treasure hunt. Reviewing the following documents can get you started in the right direction to assess the impact of an incident:

- BIA (Business Impact Analysis): Do you have a recent (completed within the last 18 months) BIA?
- RTO: Do you have clear, documented Recovery Time Objectives (RTOs)?
- SLAs: Are there documented Service Level Agreements (SLAs) with clear timelines?
- ITIL references (Event and Incident Management procedures, in particular): Are your incident management procedures clearly defined?
- Customer expectations: Do your internal and external customers have clear *and documented* expectations?

"Routine" Emergency vs "Crisis" Emergency

Distinguishing "routine" vs "crisis" emergencies can inform your response strategy. A routine emergency[1] does not mean "easy." On the contrary, a routine emergency can be very difficult and challenging. In this context, "routine" refers to the relative predictability of the situation that permits advanced preparation. The risk presented by the situation was included in your risk profile, and you likely have been able to take advantage of lessons learned from prior experiences. Therefore, you probably have created appropriate plans, developed relevant training, and completed exercises for routine emergencies. In short, your business and technology continuity and disaster recovery plans are filled with strategies to manage them.

[1] Managing Crisis: Responses to Large-Scale Emergencies, Arnold Howitt and Herman Leonard, CQ Press, page 5

In contrast, a "crisis" emergency[2] is a much different animal. These events are distinguished by significant elements of ***novelty***. This novelty makes the problem much more difficult to diagnose and then deal with. This type of emergency often have one or more of the following characteristics:

- The threats have never been encountered before, which means there are no existing plans to manage it.
- The situation may be a familiar event, however, it is developing at unprecedented speed; therefore, developing and executing an appropriate response (including notifications and ongoing coordination) is severely challenging.
- The incident may represent a confluence of forces, which, while not new individually, in combination, pose unique challenges to the response.

The novel nature of a crisis emergency becomes a game-changer. Our plans, processes, training, and exercises that may work well in routine emergency situations are frequently grossly inadequate in a crisis emergency, and may even be counterproductive. When this type of incident occurs, we realize that we have to start from scratch.

The crisis emergency also requires different response capabilities; in other words, the plans and behaviors used for routine emergencies just won't work. The first thing that must be done is to *identify* the novel elements of the event, to determine what makes this situation so different from others. Sometimes this novelty can be surprising and difficult to isolate. Teams may begin the response process thinking it is one thing and then, over time, realize it is something quite different. Even the most experienced responders can make the mistake of assuming they understand the nature of a problem based on their initial observations – a fact that clever perpetrators can use to their own advantage.

Once the real problem has been identified and people understand that routine plans won't work, the team has to improvise response measures that will be suitable to cope with the unanticipated aspects of the incident. Created out of necessity, these responses may be actions quite different than ever done before. Handling a crisis emergency may feel like you're *building* an *airplane while flying it at the same time. It's not pretty, but it may be necessary. By the way, an excellent question concerning your team skill development program is whether you have fallen into the habit of only presenting "routine" scenarios to your response teams in exercises, or do you include an occasional "this can't happen" situation?*

Lastly, in a crisis emergency, responses must be creative and, *at the same time*, be extremely adaptable as new and improvised solutions are being executed. Teams have

[2] Ibid, page 6.

to be on “full alert” at all times, as it’s not known how the situation will change, and everyone must be prepared to shift or dart at a moment’s notice. All of this makes people quite anxious, and during an incident, this anxiety often manifests itself in various ways, like excessively loud voices or hushed voices, frantic activities, and nervous laughter.

Escalation Into the Organization

Once the situation is recognized as being “bigger than a breadbox,” how is it escalated into the rest of the organization? Your IT environment may have the best internal escalation process ever created, but how does it fit into the whole organization? Many IT groups do well with internal communications, but run into problems when others in the company need information.

Right off the bat, here are three things needed to help the IT department be successful in a crisis emergency:

1. **Corporate Incident Management Team:** This team must know their roles, responsibilities, and communication options.
2. **Corporate Incident Assessment:** The team must have a clear incident assessment process, team, and escalation strategy that works for a broad-reaching incident with impact.
3. **Incident Action Plan:** The IT team must know how to develop an incident action plan and relate that to the overall company incident action plan.

Corporate Incident Management Team

Your company’s Corporate Incident Management Team (CIMT) is charged with the overall recovery of the company and its key functions following any disruptive event. IT should play a key role on the team. Know in advance the following:

- The members of the company’s Incident Management Team.
- Their roles and responsibilities.
- How they communicate.
- Where they meet.

All of this should be documented in the Corporate Incident Management Team plan and, ideally, exercised at least twice a year. And, of course, IT should play a central role on that team.

The type of incident being discussed in this article is one that reaches beyond the IT department; rather, it speaks to a corporate issue, needing the attention of the Corporate Incident Management Team. In a technology based problem, the situation can rapidly

escalate to a company-wide crisis, therefore the corporate team and IT teams need to be in sync.

Incident Assessment

Once it is recognized that the technology incident needs to be escalated beyond IT, do you know where your team would "plug in"? This should be clearly delineated in advance. Hopefully, an IT representative is part of the routine assessment process. This corporate team is often called an Incident Assessment Team (IAT).

Once the corporate Incident Assessment Team convenes, the person who knows the most about the incident would share "situational awareness." Obviously, if the situation started as a technology issue, someone in IT would be providing this information. This person should also answer questions regarding impact. Then the IAT team as a whole should review the escalation criteria. It doesn't need to be complex; the team just needs to discuss six basic areas:

1. **Technology.** Is there an impact to critical systems especially those that are external facing?
2. **Lost revenue.** Will this incident result in lost revenue, fines and missed opportunities?
3. **Production line.** Are any of our mission-critical, time-sensitive processes at risk?
4. **Reputation or brand.** If this incident is not managed well, could it impact our reputation or brand?
5. **Life safety.** Is there an impact to people? Are lives at risk? People hurt or killed?
6. **Facility.** What is the impact to our facilities? Emergency responders present?

Items one through four are very objective and can be easily discussed based on the situational awareness. The fifth, reputation/brand, is more subjective.

The IAT team then makes the decision as to whether or not the plans and teams are to be activated.

Incident Action Plan

Okay, so the Corporate Incident Assessment Team made the decision to activate. Now what? In many companies, the *Initial Assessment* Team often becomes the *Incident Management* Team (sometimes adding or subtracting a few members), and one of its first actions as an IMT should be to develop an Incident Action Plan (IAP). These simple plans are powerful. They clearly state tactical objectives with clear assignments and a designated time (known as the operational period) to come back and check in about status. This isn't rocket science – and yet most teams do not develop one, or if they do, they don't communicate it beyond a few people.

The entire process has five easy steps.

1. Assess the incident situation and report the current status of the event.
2. Establish tactical incident objectives.
    - Ensure that necessary resources are available to complete the tasks.
3. Assign all objectives (to a team or individual).
4. Determine the operational period (when the team will meet again).
5. Communicate the plan to all identified stakeholders.

These plans can be used to communicate to all key stakeholders about the incident, the status, and the plan of action.

Company Wide Incident Communication

It is also critical to think carefully about company wide incident communication. What tools are used to communicate with all of the different team members dealing with the incident or managing its impact? How quickly can you ramp up to notify everyone that needs to hear about what is going on? Depending on the incident, communication tools may be limited. Our clients that have third-party or outsourced emergency notification systems (ENS) are ahead of the game. The big plus for them is being able to use their ENS for the following activities:

- Pushing information: Pushing information to employees about the company status, and providing talking points and other key pieces of information.
- Establishing conference bridges: Using toll-free ENS conference bridges for employee, vendor, senior management, Board of Directors, and other key stakeholder phone calls.
- Assigning stakeholder groups: Using pre-defined groups for all key stakeholders to push information via phone, text or email.

If you have an ENS but only use it for a limited set of contacts (i.e., your employees), you may be surprised to discover that there is a lot more that it can be used for. Get the most out of your money by using your ENS for as many things as make sense.

Fitting It All Together

All this information is nice, but how *do* you escalate an incident? Well, in a perfect world, IT would be a presence on the Corporate Incident Management Team, and would give them a heads-up that something has happened in the technology environment that may need corporate attention. In this perfect world, the CIMT would have some type of

mechanism to identify when they would be notified and when the situation needs escalation.

Going Forward

Where do you go from here?

- Go back and revisit your internal incident assessment, action planning, and communication processes.
  - Are they sufficient for a “routine” emergency?
  - Are they adaptable for a “crisis” emergency?
- How does your process fit into the bigger organizational process?
  - If you don’t see good IT connections to the overall company incident process, share the ideas discussed today. See if you can engage the Corporate Incident Management Team to change the assessment and management process to be more inclusive.
- Get started to ensure that your IT procedures can address outages with organizational system-wide impacts.

Time is a’wasting… Your next big outage could be around the corner!

About Everbridge

Everbridge provides a unified critical communication suite that helps clients be better prepared, make better decisions, and respond quickly and confidently during disruptive events. When an incident happens, whether it's a natural disaster or an IT service outage, we automate communications to ensure that the right messages get to the right people at the right time.

Widely recognized by analysts as the market leader, Everbridge solutions are trusted by clients in all major industries and government sectors to connect with over 50 million people around the world.

THE ONLY END-TO-END PLATFORM

- **Planning**: Everbridge is easy to set up, maintain, and organize, meaning that you're always ready for a quick, coordinated response. Everbridge ensures that the right messages get to the right people - with the most advanced opt-in portal on the market, streamlined integration with internal and external data sources, and simple group and contact management.

- **Assessment**: When trouble strikes, you need rich insight, presented simply - so you can quickly assess potential impact and make an informed decision to avoid loss. Everbridge offers the only solution on the market that meets these demanding requirements, with the most advanced interactive dashboard in the industry.

- **Response**: In critical situations, ease-of-use can mean the difference between an effective response and a mistake that carries serious consequences. Everbridge is engineered to be simple to use under pressure, with a user interface that accelerates time-to-message and reduces the likelihood of errors.

- **Delivery**: Even during large-scale disruptions, Everbridge stays on. The most advanced platform in the industry ensures that you reach your contacts - every time. And with worldwide coverage and capabilities, including globally local calling infrastructure and data storage, we're ready to support you wherever your people are in the world.

Visit www.everbridge.com to learn more.