SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Program Best Practices > Resilience >

It Happens. Are You Prepared to Respond?

By the Security Executive Council

Business scandals and executive misbehavior. Cyberattacks and privacy breaches. Food contamination. Gas pipeline incidents. Natural disasters.

It may seem easy to pick out which of these things could have an impact on your organization and which couldn't. But we'd encourage you to look again.

Often, companies prepare only for likely events that could directly impact their facilities. But what about the unlikely yet quite possible – the Hurricane Harveys, the California Camp Fires, the employee misconduct scandals, the Petya attacks? What about the indirect but critical impact of disrupted supply chains that originate nowhere near your facilities?

What about the events that you wouldn't necessarily deem catastrophic, but that have the potential for significant shareholder impact? The power and immediacy of social media can elevate even a smaller operational issue to a much higher level of reputational criticality. A 2018 study called Reputation Risk in the Cyber Age shows shareholder value went up by 20% for organizations that responded well to critical incidents on social media and down by 30% for those who didn't respond particularly well.

Here are some further insights from SEC emeritus faculty members Alan Borntrager (former affiliation: Red Hat) and John Slattery (former affiliation: BAE Systems), Ray Gerwitz (Executive Director & Deputy CSO, UT Police at U of Texas MD Anderson Cancer Center & U of Texas Health Science Center) and SEC Managing Director Bob Hayes on how to successfully prepare for and manage critical incidents of all types.

Rehearse

Drilling critical incident response plans may draw complaints of unnecessary cost and time. But without rehearsal, even a good plan will overlook issues that can compromise safety and efficiency on the ground during the event.

- Base the frequency and depth of your drills upon the size of your organization, its

culture, the extent of executive support, and your geographic footprint. Consider coordinating your plan with neighboring organizations and invite them to drill with you, especially in mixed tenant facilities.
- Participate in public-private emergency response exercises. Where possible, reach out to offer your facilities and resources to public partners.
- During the rehearsal phase, remember that relationships are more valuable than MOUs. Formal agreements with public entities build confidence, but when the event arrives, the cell number of the right individual responder will be much more valuable.

Build a Multidisciplinary Team

Some of your essential resources will reside outside of the security team.

- Drill down and understand the relationships that could exist between nontraditional partners beyond environmental health and safety and public safety.
- Audit, HR, IT, and Supply Chain should be considered in the emergency response and critical incident plan.
- Make sure there is someone – the security leader or someone else – who sets the rules and boundaries for the whole multidisciplinary team. Each role needs to clearly understand when the baton will be passed to them – when is it their job to respond?

Understand the Elements of Crisis Leadership

Good crisis leadership requires you (and your organization) to

- respond immediately,
- know the facts,
- act decisively and quickly
- stay focused,
- respond globally, and
- make amends.

Your duty of care for the employees and families of your organization, as well as for other victims of a critical incident, requires your responses to be communicated with sensitivity, compassion, honesty and courage.

Further, security and business continuity leaders need to be ready to stand alone. Public law enforcement will likely have to be pulled away to deal with public safety issues, so whatever assistance they provide in your organization may not be available.

Communicate Internally and Externally

Internally:

- Ensure that all individuals involved in your incident command framework know who is next in command and communicate that to all impacted parties both within and outside of the emergency response team.
- Have backups and contingencies in place for communications, with preferred methods identified and tested for Primary, Alternate, Contingency and Emergency (PACE) communications.

Externally

- Ensure that someone in the organization is in charge of engaging in social listening and rapid response on social media platforms. Again, make sure your voice is calm, knowledgeable, and compassionate.

Be Adaptable

Be specific in your critical incident response plans – include targeted checklists and detailed resources. But don't inhibit your on-site teams' authority to act decisively and flexibly as they're responding to unexpected events. No procedure can confront all the complexities that may arise.

Remember there will be individuals in the organization who will want to rely on and defer to the established frameworks of decision making in the organization because they don't want to get outside their comfort zone. Some people may need to be trained to respond adaptively. Also recognize Security may not always be the designated leader on paper, but during a critical incident, they invariably end up serving in that role as others default to them as the event is unfolding.

Always Care for People

Staff and responders who are worried about their own families and homes during an event will not be able to give their all to helping the organization respond.

- Poll your team and other employees of the organization regularly to find out what their needs are during the critical event and how you can help take care of their homes and families
- Plan for the operational impact of extended periods of strain. If an event continues over multiple days or weeks, it will have an additional strain on your people that may impact their performance in recovery.
- Remember that victims of events may take four to six weeks to regain equilibrium. Be patient and continue a culture of care over that time.

Know How to Demobilize

Think about how you will exit a critical incident. If an emergency requires personnel to be working 12-hour shifts over the span of the event, make sure that you are planning in staffing and time to allow those personnel to recover sleep and manage personal issues before returning to the normal operational tempo.

Visit the Security Executive Council web site to view more resources in the Program Best Practices : Resilience series.

About the Security Executive Council

The SEC is the leading research and advisory firm focused on corporate security risk mitigation solutions. Having worked with hundreds of companies and organizations we have witnessed the proven practices that produce the most positive transformation. Our subject matter experts have deep expertise in all aspects of security risk mitigation strategy; they collaborate with security leaders to transform security programs into more capable and valued centers of excellence. Watch our 3-minute video to learn more.

Contact us at: contact@secleader.com
Website: https://www.securityexecutivecouncil.com/

