

When Business Continuity Events Becomes Crises: The case for an integrated, flexible system that scales with crisis



The challenges to effective business continuity management have only gotten worse

The Covid-19 crisis has painfully laid bare many of the longstanding challenges to effective business continuity management practices that continuity managers face on a daily basis. The list itself is disturbingly familiar, beginning, of course, with a lack of executive buy-in impeding comprehensive business continuity planning.

Indeed, the data bears this out. Even as the risk of business disruptions increased over the years, surveys continued to point to a stubborn lack of preparation: in IBM research, fewer than 20 percent of business continuity management and IT security specialists could claim that their organizations had a formal business continuity plan. Meanwhile, 73 percent of organizations acknowledged not doing enough to insulate themselves from disaster and ensure business continuity at all times, according to a Disaster Recovery Preparedness Council surveyⁱ.

Early numbers from the Covid-19 response tell a similar tale. In a wide-ranging survey of the business continuity impacts of the coronavirus pandemic, a mere 37 percent of companies said they had the right technology in place for employees to conduct critical business operations from home in the event of an emergency. And nearly 20 percent of companies admitted that none of their workers could do their work from home due to a lack of technology equipment owned and distributed by the businessⁱⁱ.

Even organizations who could make the transition to a largely remote workforce confronted latent business continuity challenges when they did – one major issue being the inability to reach fragmented, distributed workforcesⁱⁱⁱ. Cited as an emergent business continuity challenge at the end of 2018, this inability to reach remote staff results from the lack of both up-to-date, employee contact information on file as well as emergency notification technology to enable two-way communication between employer and staff^{iv}. Perhaps tenable during a short-term business interruption, the inability to consistently reach employees – a latent continuity problem – has only burgeoned into a full-bore crisis for many companies responding to the Covid-19 pandemic that has further precipitated the geographical fragmentation of the workforce.

Indeed, this example highlights the innate difficulty in maintaining a constant state of preparedness for even the best-resourced business continuity teams. And therefore, this guide, attempts to demonstrate how slight changes in the way business continuity teams are resourced can immeasurably enhance the function's ability to improve operational resilience.

Time-bound disruptions become longstanding crises

It starts with considering the different tools and techniques that might enable continuity managers to achieve core continuity objectives. You see, because the goal of business continuity management is to restore organizations to a state of “business as usual” as quickly as possible, there is a widespread belief that continuity professionals only require operational tools and techniques (e.g. plans, checklists, etc.) to deal with time-bound disruptions.

Nor is that belief without support. After all, the business continuity management lifecycle – identify, analyze, design, execute, and measure – is itself overwhelmingly linear; why shouldn't management techniques be, as well?

Meanwhile, it has largely fallen to crisis management, especially in larger organizations, to respond to abnormal, unstable situations. These situations, chronic, persistent crises, tend to be of longer duration than incidents or disruptions. They, therefore, have necessitated a more “evolutionary” lifecycle – signal detection, searching and reducing, damage prevention, recovery, reviewing and critique^v - and management techniques (e.g. collaboration tools, incident reports, etc.).

Why, then, do these distinctions even matter if each function uses the tools and techniques relevant to its specific lifecycle? Well, the truth is what begin as time-limited incidents often, in fact, beget crises – just look at two of the traditional causes of crises, as argued by the British Standards Institution, that have strong roots in time-limited incidents:



Those stemming from poorly managed incidents and business fluctuations that are allowed to escalate to the point at which they create a crisis.



The emergence of latent problems with serious consequences for trust in an organization's brand and reputation. Problems can incubate over time, typically as a result of:

- A lack of governance allowing gradual and incremental slippages in quality, safety or management control standards to go unchecked and become accepted as a normal way of working.
- Convenient, but unofficial, “workaround” strategies becoming the normal routine due, for example, to overcomplicated processes, unrealistic schedules, chronic personnel shortages and lax supervision.

- Flaws in supervision and process monitoring, which promote an expectation of “getting away with” undesirable behaviors or being able to survive minor failures without reporting them, or over-reliance on controls to catch all errors, rather than an expectation of quality checks that catch only occasional problems.
- Blame cultures that encourage risk and issue cover-ups and the lack of a shared sense of mission and purpose, which generate a defensive (if not actually hostile) “them and us” attitude between staff and management, between different parts of the organization and between the organization and external interested parties.
- Poor training and development of staff and managers, or incremental loss of skills and knowledge^{vi}.

Not just that, latent continuity issues (i.e. inability to reach a globally distributed staff) quickly become chronic crises with an external trigger. As such, the failure to plan for the likelihood that incidents and issues can become crises will only impede an organization’s ability to return to business as usual. For instance, the plurality of companies have business continuity plans that cover emergency operations for a maximum of three weeks^{vii}.

Incidents or crises: How the two concepts differ?

The distinction between incidents and crises might seem like an academic point. But understanding how incidents can spiral into crises can help continuity teams respond to both sets of events, thereby returning their organizations to a business as usual sooner.

Characteristics	Incidents	Crises
Predictability	Incidents are generally foreseeable and amenable to pre-planned response measures, although their specific timing, nature and spread of implications is variable and therefore unpredictable in detail.	Crises are unique, rare, unforeseen or poorly managed events, or combinations of such events, that can create exceptional challenges for an organization and are not well served by prescriptive, pre-planned responses.
Onset	Incidents can be no-notice or short notice disruptive events, or they can emerge through a gradual failure or loss of control of some type. Recognizing the warning signs of potential, actual or impending problems is a critical element of incident management.	Crises can be sudden onset or no-notice, or emerge from an incident that has not been contained or has escalated with immediate strategic implications, or arise when latent problems within an organization are exposed, with profound reputational consequences.
Urgency and pressure	Incident response usually spans a short time frame of activity and is resolved before exposure to longer-term or permanent significant impacts on the organization.	Crises have a higher sense of urgency and might require the response to run over longer periods of time to ensure that impacts are minimized.
Impacts	Incidents are adverse events that are reasonably well understood and are therefore amenable to a predefined response. Their impacts are potentially widespread.	Due to their strategic nature, crises can disrupt or affect the entire organization, and transcend organizational, geographical and sectoral boundaries. Because crises tend to be complex and inherently uncertain, e.g. because a decision needs to be made with incomplete, ambiguous information, the spread of impacts is difficult to assess and appreciate.
Media scrutiny	Effective incident management attracts little, but positive, media attention where adverse events are intercepted, impacts rapidly mitigated and business-as-usual quickly restored. However, this is not always the case and negative media attention, even when the incident response is effective and within agreed parameters, has the potential to escalate an incident into a crisis.	Crises are events that cause significant public and media interest, with the potential to negatively affect an organization’s reputation. Coverage in the media and on social networks might be inaccurate in damaging ways, with the potential to rapidly and unnecessarily escalate a crisis.
Manageability through established plans and procedures	Incidents can be resolved by applying appropriate, predefined procedures and plans to intercept adverse events, mitigate their impacts and recover to normal operations. Incident responses are likely to have available adequate resources as planned.	Crises, through a combination of their novelty, inherent uncertainty and potential scale and duration of impact, are rarely resolvable through the application of predefined procedures and plans. They demand a flexible, creative, strategic and sustained response that is rooted in the values of the organization and sound crisis management structures and planning.

The benefit of integrated, crisis and continuity software that scales

What, then, can be done? As mentioned, crisis and continuity managers might be used to responding to events of different scale and complexity with different tools and techniques. But when the event itself begins small and time-limited and becomes larger and longer standing, it is imperative that the software platform used for the original response scales to address the latter. Otherwise, valuable time will be wasted, hindering the ability of either response team to achieve situational awareness.

What's needed, specifically: teams should be looking to manage all aspects of business continuity and crisis management in a unified preparedness and incident management platform, mobile and scalable, so as to effectively assess business risks and impact, coordinate responses to disruptions, as well as manage incidents from the smallest outage to a major crisis. But not all software is created equal. The following considerations apply when procuring ISO 22301-compliant continuity management software that scales with events in real time:



Situational awareness and collaboration.

A solution that already lets Continuity teams visualize the locations of specific risks (also, incidents, people, and assets) with fully integrated mapping features will serve to clear a critical path to situational awareness during the actual incident. To further support better visibility and awareness outcomes, as well as facilitate communication and collaboration, the flexible system should also include chat, impact, assessment, and communication planning functionality. What's more, the software should enable teams to communicate and follow-up within the app itself, preferably via dedicated, event-specific chat rooms, in addition to email, SMS, and app notifications. Additional, advanced features to improve collaboration include dashboards and collaboration spaces which provide teams with key details, actions, feeds, and timelines.



Automated response.

In the event of an escalating crisis, unified preparedness and incident management software should help continuity managers set up and activate crisis and incident management teams, including structures, roles, capabilities required, and on-call resources. Once those teams are up, running, and responding to high-impact events, the software should also help manage incident response tasks, log and share updates, decisions, facts and assumptions, as well as produce situation reports and briefings. To facilitate this level of response, the platform should provide fully-configurable workflows that automate and lead people through pre-set procedures, as well as set recovery targets for business activities and automate reporting on those targets as the incident evolves.



Planning and review.

Teams simply can't adequately respond to critical events without first activating tested, best-practice plans and strategies. Nor can they appropriately recover from critical events without documenting and internalizing lessons learned. Unfortunately, that's where most BCM software falls down: too little planning and review-related functionality. Your solution needs to provide a comprehensive library of crisis and incident response plans and teams structures, covering anything from common disruptions to hazards scenarios.

The mobile-friendly platform should also be able to digitize business continuity, crisis, and incident response plans, including strategies and considerations, roles and responsibilities, as well as pre-assigned checklists that are ready to deploy when incidents do occur. Testing is equally important; so, when events do occur, those plans come to life seamlessly and teams know what they need to do, and progress gets tracked in real time. Software should help there, too, by enabling teams to conduct routine exercises.

And don't neglect the recovery stage of the management lifecycle. Here, effective software functionality should facilitate post-incident reviews and lessons learned. That way valuable insights go back into best-practice continuity plans for next time.

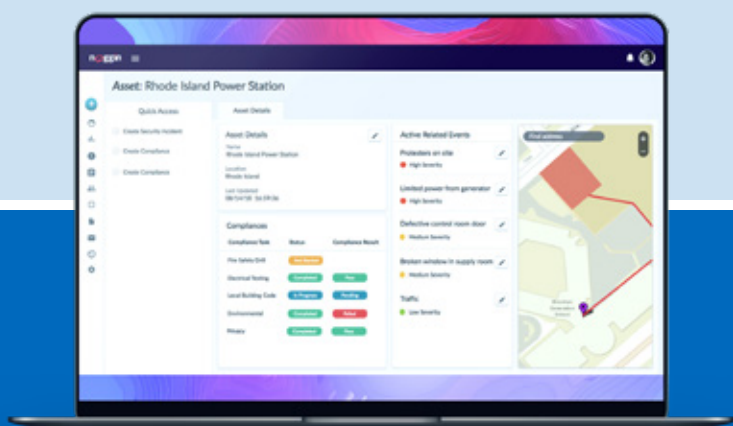
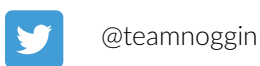
Finally, the Covid-19 crisis has surfaced many of the long-simmering challenges with developing and sustaining effective business continuity management practices, with one of the most latent challenges being the inability to plan for disruptions that morph into protracted crises. Fortunately, unified preparedness and incident management software platforms, like Noggin Continuity, provide business continuity management best-practice compliance, like ISO 22301, alongside other flexible capabilities needed to effectively assess business risks and impact, coordinate responses to disruptions, and manage incidents from the smallest outage to a major crisis.



Citations

- i Providence Journal: Global Benchmark Study Reveals 73% of Companies are Unprepared for Disaster Recovery. Available at <https://www.providencejournal.com/business/press-releases/20140304-global-benchmark-study-reveals-73-of-companies-are-unprepared-for-disaster-recovery.ece>.
- ii Todd R. Weiss, Tech Republic: Business continuity plans and tech are lacking during the coronavirus pandemic. Available at <https://www.techrepublic.com/article/business-continuity-plans-and-tech-are-lacking-during-the-coronavirus-pandemic/>.
- iii Ann Pickren, Security Magazine: Five Emerging Business Continuity Challenges For 2019. Available at <https://www.securitymagazine.com/articles/89676-five-emerging-business-continuity-challenges-for-2019>.
- iv Ibid.
- v Jose Sarriegi et al., Universidad de Navarra: The Dynamics of the Crisis Lifecycle for Emergency Management. Available at https://www.researchgate.net/publication/255643967_The_Dynamics_of_Crisis_Lifecycle_for_Emergency_Management.
- vi British Standard 11200: 2014. Crisis Management. Guidance and Good Practice.
- vii Todd R. Weiss, Tech Republic: Business continuity plans and tech are lacking during the coronavirus pandemic. Available at <https://www.techrepublic.com/article/business-continuity-plans-and-tech-are-lacking-during-the-coronavirus-pandemic/>.

Like what you read?
Follow Noggin on social media



noggin

for Business Continuity

Meet the next-generation tool for corporate crisis and business continuity management teams to collaborate, plan, track their response, and share information. Built on the Noggin Core platform, Noggin Business Continuity gives response teams and decision makers the tools to know what's happening, collaborate quickly and effectively, make better decisions, and enact the right plans to take action when it counts the most.

The Noggin Business Continuity solution pack is backed by the Noggin Library with hundreds of plans and best-practice workflows, out of the box, and installed in minutes.

To learn more,
visit: www.noggin.io
or contact: sales@noggin.io