noggin

A Buyer's Guide to Critical Event Management Software

The escalating critical event threat exacerbates response and coordination challenges

The world hasn't been this volatile in a long time. Just consider the cascade of crises we confront today – emerging COVID variants and subvariants, geopolitical conflict in eastern Europe and the western Pacific, civil unrest, cyber threats, supply chain disruptions and staffing shortages, rising inflation, and natural disasters.

And these are just the known threats we face concurrently. More and more often, unexpected crises emerge one after the other, compounding individual impacts and hindering our ability to respond effectively.

Not just that, the ongoing pandemic has made responding to individual disruptions more difficult than ever.

For one, workforces have become geographically fragmented. UK data shows that almost a third of businesses aren't certain what proportion of their employees will be working remotely in the future[i].

Why that matters? It's more difficult to protect employees working alone and/or in remote locations, especially since the employer duty of care obligation remains operative wherever the employee works.

That's not the only challenge to effective business continuity and crisis and emergency management. Workers today are also inundated with constant messaging, thanks to the rapid uptake in corporate communications tools.

These collaboration technologies might improve productivity and (remote) engagement. But they also make it harder for crisis and emergency communications to break through when it matters most. Those messages need to be consumed and acted upon immediately.

Then, there's the data privacy challenge to effective business continuity and crisis and emergency management. With workers so geographically fragmented, employers need more granular data about their workers' physical whereabouts.

Employers, however, must go through (escalating) compliance hoops to obtain actionable data about their employees, as most advanced economies now enforce stringent data privacy regulations.

For instance, the world's largest economic bloc, the European Union, has one of the strictest data privacy frameworks of all, the General Data Protection Regulation (GDPR). California, the largest state economy in the US, has modelled its data privacy laws on the GDPR.

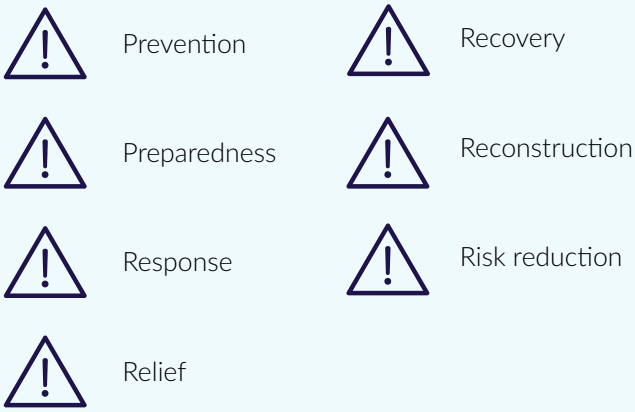
The practical effect of these laws is the strict regulation of corporate data. Which often complicates the task of making effective use of employee data, including location and contact details, to ensure safety in the event of an emergency.

The need for critical event management in an age of escalating crisis

Given the threat climate and resultant challenges, what can organisations do to mitigate the impact of critical events likely to come their way? The traditional mechanisms of business continuity as well as crisis and emergency management won't be enough.

Certain experts have acknowledged the fact. Senior officials in the Australian Government, for example, have pushed for an "all-hazards" approach to managing that country's risks holistically.

To that end, the Australian Government revised its Crisis Management Framework (in 2021), endorsing a novel seven-phase continuum for disaster management and recovery. The phases include:



Nevertheless, many legacy structures for addressing critical threats, having long been too focused on individual emergency risk, aren't up to the task of implementing such an all-hazards approach. What can be done?

That's where critical event management comes in.

An all-hazard's approach to addressing the crisis threat, critical event management is about managing preparation, response, and recovery from events that impact continuity, operations, and safety. In this way, critical event management intersects incident management, emergency response and communications, risk intelligence and management, as well as crisis management and business continuity.

The benefits of such an all-hazard's approach (over one siloed off in IT) are clear. Indeed, critical event management efficiently aligns inter-departmental (or agency) resources to respond to disruptive incidents. This work includes teaming up stakeholders from relevant departments and business lines, improving inter-departmental (or multi-stakeholder) coordination and communication flows, integrating necessary processes, and post-hoc reporting and analysis.

Further, effective critical event management gives business leaders a dynamic, consolidated view of threats, automated functionality to assess and respond to those threats, as well as information capture capabilities for critical event reporting.

Other business benefits of critical event management include greater operational efficiency (from fewer system and process redundancies), reduced costs, improved situational awareness and visibility, as well as better post-hoc reporting that leaves a valuable audit trail.

The need for critical event management software

Of course, these benefits don't just materialise. Organisations must first be serious about building up their resilience and business continuity capabilities, to implement critical event management strategies.

Then, firms must act expeditiously. Often, organisations delay implementing needed changes in all-hazard's risk management until a new crisis emerges.

By then it's too late. As many have learned the hard way, implementing new resilience and continuity frameworks in the middle of a critical event is a recipe for disaster.

What can organisations do, instead?

Here, critical event management software comes in handy. These are software solutions and related services designed to manage an institution's preparation, response, and recovery from events that impact continuity, operations, and safety.

Not just high-impact events, either. Critical event management solutions can help organisations handle lower-impact events and critical issues, too. That gives the organisations that procure these solutions an advantage, i.e., they can use the same tools to manage routine, smaller issues as they do for larger impact events.

So, what are the core components of these solutions? According to independent analysts[ii], fundamental features of critical event management software include:

Emergency mass notification tools for targeted communications. Enables effective crisis and emergency communications to impacted individuals and response teams. Offers the benefit of both increasing response efficiency and reducing the risk personnel faces during critical events.

Employee-tracking to maintain duty of care. Enables the identification of threats to relevant personnel wherever they are. Personnel can leverage these capabilities if they find themselves threatened or during critical events to alert employers of their status.

Incident management to improve the efficiency of emergency response. Serves as centralised hubs, or virtual emergency operations centres, to process incoming situational and risk data and manage the response effort. Offers response teams an in-depth view into critical events.

Capabilities to consider when procuring critical event management software

Of course, developments in proactive critical event management software aren't happening in a silo. Technology trends, such as interfaces and experiences as well as business and productivity enablers, are entering critical event management from the larger world of digital innovation, with each making a significant impact on innovative offerings on the market today.

As a result, shrewd technology buyers are turning their backs on single use, point solutions, whether for communications, collaboration, or information capture.

Instead, sophisticated buyers are looking for management systems and multiple use case solutions (inclusive of business continuity as well as crisis, emergency, safety, and security management) to ensure continuous improvement.

Within that software market, what innovative capabilities to look out for? We recommend the following:

Crisis management

- **Crisis response.** Advanced solutions should apply best practices to plan for, respond to, and manage critical events and exercises. Built on international standards, such as ISO 22398, the solutions should also enable faster response, better collaboration using plans and playbooks, smart workflows, and real-time dashboards and insights, ensuring better incident response, decision-making, and continuous improvement.
- **Incident response plans and checklists.** Best-practice libraries should come included. That way organisations can easily create crisis strategies and action plans for different types of events that define the required strategy, action items, completion time targets, and people involved.
- **Crisis communications.** Single platform, multi-use case systems should help organisations manage complex communications, centralising, approving, and standardising their crisis response. They should also provide effective communication pathways for all aspects of incident management.

Emergency management

- **Emergency response.** These tools should provide all that is needed to manage any incident effectively, following ISO, ICS, and other national standards. They should keep your whole team following the same plans, communicating on the same platform, and viewing the same operating picture - from any place or device.
- **Incident and resource mapping.** These systems should come equipped with powerful mapping tools to create multilayers maps, integrating both external feeds and any information housed within the platform.
- **Operational cycle management.** These systems should support the battle rhythm of response operations, understanding and tracking reporting periods.
- **Community lifeline monitoring.** These systems should provide executive-level insight into safety threats to the public and to staff, by regularly assessing community lifelines.
- **Incident and exercise management.** With these solutions, it should be easy to manage incidents and run exercises, as well as record post-incident reviews and lessons learned to improve the response. The solutions should also enable you to escalate any business continuity incident into a crisis seamlessly.

Business continuity

- **Critical infrastructure protection.** Innovative solutions should keep up with the escalating risk to key assets, assessing those risks in advance and monitoring critical facilities throughout the emergency response process.
- **Welfare checks.** The solutions should enable organisations to send welfare check messages to their event response staff or any other type of contact. Organisations should also be able to collect replies, to identify who needs assistance and prioritise follow-up actions.
- **Critical dependencies tracking.** With these solutions, you should be able to quickly identify dependencies between business activities and supporting assets or vendors and stay informed when one is at risk.
- **Recovery strategy tracking.** The systems should enable you to collect and aggregate data to highlight any critical activities, processes, assets, and resources lacking recovery strategies, or untested recovery strategies that put your business at risk.

- **Standards compliance.** The systems should be able to monitor compliance against, ISO, legislative, and crisis industry standards, storing all compliance data in one place.
- **Audits and inspections.** You should be able to manage crisis audits and inspections easily, using a Library of templates to get you started fast. You should also be able to make templates your own, adding unique requirements and other additions if needed.
- **Cyber threats and treatments.** These solutions should let you manage cyber threats and treatments in a consistent, systematic, and easy to use manner, starting with a library of 20 standard threats and 171 treatments. You should also be able to assess threats for inherent, target, and residual risk severity levels, approve assessments, and rate controls for effectiveness. You should also be able to schedule risk assessments for periodic review and generate ad-hoc reports to monitor the review process.

Finally, the era of multi-directional threats is here, with crises likely to remain concurrent, consecutive, and compounding. And so senior leaders must ask themselves, what can they do to keep their organisations solvent and their people safe?

The evidence suggests that getting serious about critical event management strategies is the only way.

Advanced critical event management solutions, as such, will be key to implementing those strategies. Integrated platforms, like Noggin, give you all the tools and information needed to manage any event effectively through its entire lifecycle of mitigation, preparedness, response, and recovery.

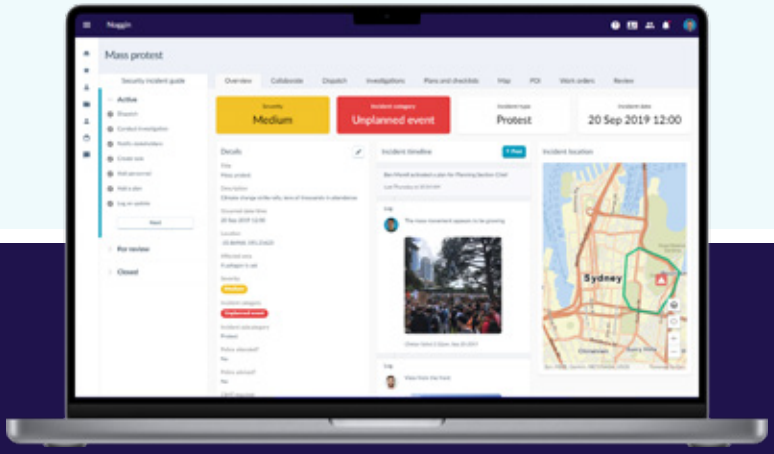
The result of keeping the whole team following the same plans, communicating on the same platform, and viewing the same operating picture: maintaining and enhancing business resilience by staying ahead of the innovation curve.

Sources

i. *Connor Taylor with Rodolphe d'Arjuzon, Verdantix: Smart Innovators: Critical Event Management.*
ii. *Ibid.*

Like what you read? Follow Noggin on social media

@teamnoggin facebook.com/teamnoggin linkedin.com/company/noggin-it



noggin

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

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 Solutions 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 Solution pack is backed by the Noggin Library with hundreds of plans and best-practice workflows, out of the box, and installed in minutes.