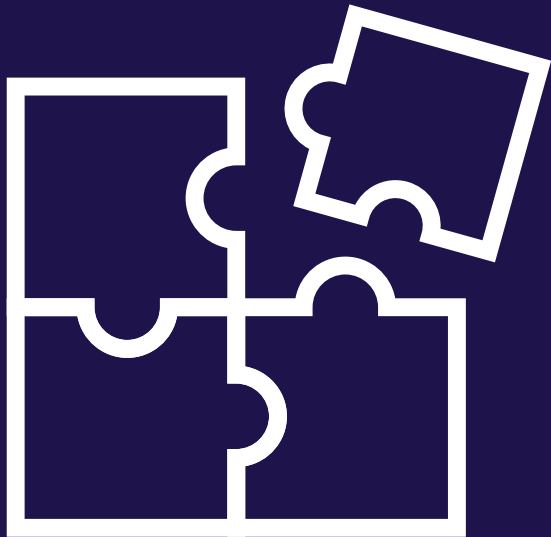


The ROI of Business Resilience Strategies and Critical Event Management Software



COVID-19 pushes traditional sources of competitive advantage aside

Product differentiation, pricing, and strategic acquisitions have long been the sources of competitive advantage that senior leaders seek.

However, COVID demonstrated that all the brilliant hires in the world won't keep your doors open when a major crisis comes through and you're unprepared.

Indeed, companies need to be able to withstand prolonged periods of acute disruption or all prior competitive actions will be rendered moot.

And these periods of disruption are increasingly becoming the norm; look at the crises we face – exotic infections, war in eastern Europe, the prospect of hostilities in the western Pacific, major trade conflicts, civil unrest, cyber-attacks, supply chain disruptions and staffing shortages, inflation, and natural disasters.

Entering this new normal of increased crisis risk, companies now need to establish a solid base of business resilience, to secure a competitive advantage in the market.

How are they going about it?

The state of business resilience

Data shows that some progress is being made. Business leaders, for their part, have finally recognized that effective business resilience strategies and protocols can make the difference between faltering or flourishing.

In fact, seven in ten organizations report planning to increase their investments in building resilience; among risk officers, the numbers are even higher – nine in tenⁱ.

That's according to the latest Global Crisis Survey put out by PWC. In it, 95 per cent of responding business leaders acknowledge that their crisis management capabilities need improvementⁱⁱ.

Sure, business leaders are finally awake to the issue. However, they dug themselves into a resilience hole that COVID only deepened.

How so?

In the pre-COVID times, too many organizations pursued business resilience as spreadsheet exercises. What followed when crisis struck: only 35 per cent of companies had very relevant crisis response plansⁱⁱⁱ. More than 30 per cent didn't even have designated core crisis response teams, according to PWC.

As a result, a staggering 70 per cent of companies now say that their business was negatively impacted by the ongoing crisis^{iv}.

7 in 10 organizations report planning to increase their investments in building resilience; among risk officers, the numbers are even higher – **9 in 10**ⁱ

According to the latest Global Crisis Survey, **95%** of responding business leaders acknowledge that their crisis management capabilities need improvementⁱⁱ

Business resilience strategies to garner a competitive advantage

The question now, is what can be done? Organizations behind the eight ball will have to hustle to develop, implement, and maintain business resilience strategies if they have any hope of competing in today's volatile market.

To do so, the senior leaders of these companies will have to step up, committing themselves to enhancing organizational resilience in the following ways:



Provide adequate resources to enhance the organization's resilience



Find mechanisms to ensure those investments are appropriate to the organization's internal and external contexts



Develop appropriate governance structures to achieve the effective coordination of organizational resilience activities



Invest in systems that support effective implementation of organizational resilience activities and arrangements to evaluate and enhance resilience in support of organizational requirements



Pursue effective communications to improve understanding and decision making

Even with the best leadership, however, not much will get accomplished without the right people in the right roles. To this end, senior leaders must develop and encourage a crisis response team within the organization to lead under a range of conditions and circumstances, including during periods of uncertainty and disruption.

This team will be mobilized to execute the crisis and emergency response plan to keep critical operations moving.

Of course, the team will have to design the plan first. That plan should be in alignment with the larger corporate strategy – hence, the importance of C-suite involvement in the process. The plan should also account for the important lessons learned during the COVID crisis.

The crisis team will routinely test and refine the plan, signaling to the rest of the organization that resilience is more than a check-the-box exercise, instead a new source of competitive advantage in the form of an integrated business resilience program.

And the intent of this program will be to provide the organization a forward-looking, systematic approach that creates structures and processes, trains people to work within them, and is evaluated and developed in a continuous, purposeful, and rigorous way.

Besides the crisis response team and plan, a few other constituent elements will go into the integrated resilience program, including a capacity to rehearse and rework plans. This capability serves to ensure that business resilience practices are working as planned. That's why the after-action report, the natural terminus of the (cyclical) testing process, is an important output of the integrated resilience program.

Most would have heard of the after-action report already. The post-testing after-action report does something similar, in that it (a) gives organizations an overview of the exercises and testing performed, (b) reports on any successes against performance objectives, (c) elucidates what went well, (d) lays out the issues identified, and (e) lists subsequent remediation actions to be taken and by whom.

Of course, post-testing after-action reports differ in substance from post-crisis after-action reports; the former, by definition, details what happens in the more controlled exercise environment. What, then, are discussion points one might see in the former but not the latter? Discussions might include:

- The set-up and staging of the exercise (project management versus crisis management)
 - Experiences of the participants with respect to the set-up (first impressions and the evaluation forms)
- Exercise aims or objective of testing
- Constraints on the exercises and testing process
- Exercise performance objectives
- Type of exercises and testing
- Choice of a location
- List of preparation participants
- Expert opinion concerning the quality of the exercise
- Conclusions regarding the validities of the exercise and the durability of the exercise aims
- Evaluation of the exercises and testing performances
- Recommendations for the next exercise
- Self-reflection of the participants, taking into account the adaptation of the exercise aims
- Operational performances, competencies, and learning experience of participants

The ROI of business resilience and critical event management software

Is it worth it, though? Well, the ROI of such a program, according to experts, includes (1) improved ability to anticipate and identify threats, (2) faster response activation, through visibility and clarity of roles and plans, (3) better access to critical data and insights, (4) improved trust with stakeholders, and (5) the ability to emerge stronger.

These attributes will stand any organization in good stead in this volatile business environment. As such, pursuing them systematically is key to securing a competitive advantage.

Given the current crisis climate, however, business leaders can't afford to delay the process any further. Instead, they should start now, building out the crisis response team and promoting the integrated resilience program.

Here, digital technology plays an outsized role. Specifically, critical event management technology will help organizations pursue best-practice resilience-enhancing strategies in alignment with international standards, such as ISO 22216 (Business Resilience) and ISO 22398 (Crisis Exercises and Testing).

So, what are the core components of these ROI-enhancing solutions? According to independent analysts, 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.

ROI-enhancing critical event management software capabilities


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 serving to enhance the ROI of the organizations that procure solutions who have embraced said trends.

In turn, those looking to generate outsized ROI have been turning their backs on point solutions that only offer one use, whether communications, collaboration, or information capture.


Instead, savvy buyers have been looking for integrated management systems and multiple use-case solutions, inclusive of business continuity, crisis, emergency, safety, and security management. Out of them, they get the best bang for their buck while ensuring continuous improvement.




Within the software market, what ROI-enhancing 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.

Chaos, not order, defines this volatile business environment. And if you're not adequately prepared, all prior competitive moves will be rendered moot.

Fortunately, moving towards organizational resilience is a strategic action, with excellent ROI that you can take now in alignment with your wider business strategy. Not only does it help you withstand the worst of the crisis moment, but it also enables you to emerge stronger.

Don't dawdle, though. Business resilience strategies need to be implemented expeditiously, with the help of ROI-enhancing critical event management software. These integrated management system solutions, like Noggin, give you the best bang for your buck, while ensuring better incident response, decision-making, and continuous improvement.

Sources

- i. PWC: Global Crisis Survey 2021. Available at <https://www.pwc.com/gx/en/issues/crisis-solutions/global-crisis-survey.html>.
- ii. Ibid.
- iii. Ibid.
- iv. Ibid.
- v. Connor Taylor with Rodolphe d'Arjuzon, Verdantix: Smart Innovators: Critical Event Management.



Like what you read? Follow Noggin on social media



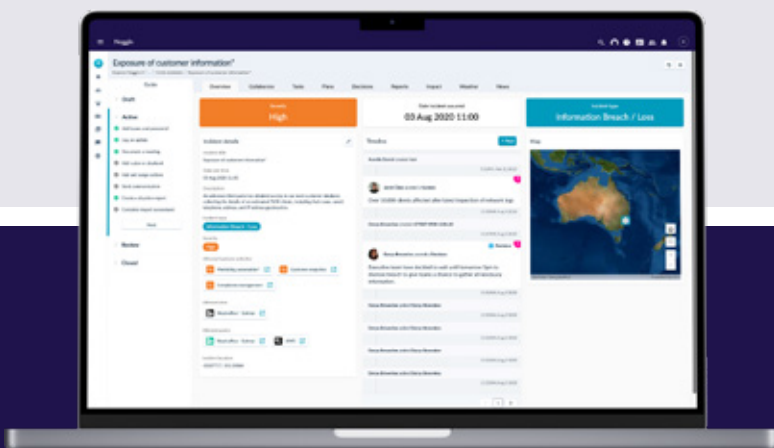
@teamnoggin



facebook.com/teamnoggin



linkedin.com/company/noggin-it



noggin for Crisis

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 Crisis 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 Crisis 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