Disaster, Catastrophe, Crisis - or Incident

The Value of Incident Management in Emergency Preparedness and Business Continuity

James Delgado, CFM, CIPS

Disaster preparedness plans can include Incident Management Plans, provisions for business disruptions well short of disasters. Plans can be designed for urgent situations of any scale but why do so? Because their use in incidents that are not disasters brings valuable familiarity, confidence, and critical reviews, substantially adding to findings and improvements from the scenarios, exercises, drills and reviews that are universally required in disaster readiness programs. Use in actual incidents is cost efficient and mitigates risk of further disruptions.

Photo by Wade Austin Ellis on Upsplash

Introduction

Catastrophe, crisis, disaster, business recovery… titles containing such terms identify plans to respond to mishaps that involve FM. Plan naming conventions and particulars of content vary with places, events, and industries. Business Continuity Plan (BCP), Crisis Management Plan, Business Recovery Plan, and Incident Management Plan (IMP) are representative titles.

The titles bring to mind disasters or major events that are very unlikely to occur. Nonetheless, such plans are essential. They require budgeting for plan maintenance, training, exercises, and reviews - always with the likelihood that they will never be used. This article turns around that perception. You can use such plans for mishaps smaller than disasters, adding strongly to their value proposition. This article advances an approach that results in familiarity with the plans for executing timely response, recovery and restoration.

Incidents - risk perspective

When a business is disrupted, there are often costs to recover and reduced revenues at the same time, leading to reduced profits, sometimes for a lengthily time. Mitigate the risk with insurance? Partially, perhaps, but the extent of losses can be hard to predict, measurable only afterward. Business Disruption Insurance seldom covers all costs and does not replace lost customers and reputation. An Incident Management Plan gives direction to leaders and team members to recover core operations then the remainder, in order. This systematic approach is the best antidote to risk of disruption by an incident well short of a disaster.

Background: vulnerability, innovation, evolution

As technology became a key driver in operating businesses, failures in these systems drew much attention on how best to keep them operating, with their capabilities and functions available. The rule of 99 percent became a target for IT availability developers due to its complications. That is, targeting 100 percent availability is straight forward. Targeting 99 percent is complicated and slippery. This launched the concept of full and rapid recovery. Managers acquired climate-controlled rooms with highly reliable component cooling, uninterruptible power, generators and fire suppression systems, and related measures in technology settings, especially in high availability data centers.

By the 2000s progress was well underway. With the horror of 911, the position of businesses and the need for more robust disaster management and recovery programs was evident. Over the years that followed these programs expanded across the globe. The depth, details and level of participation all changed, not only for large multinational companies, but smaller national and regional businesses as well sought capabilities for full and rapid recovery.

Ongoing terrorist, hacker - even espionage - threats and occurrences brought refinements and expansions to technology systems recovery. Governments, schools, churches and building operators with vulnerable business tenants built their own programs. The question became, what are the concerns that need to be addressed with each technological entity and the organizations depending on each?

Where are we now?

Recovery strategies for information technology should still be key to your programs. Business information and technology has evolved since plans first came together. Current technology enables all with suitable connections to access components such as networks, servers, desktop and laptop computers and wireless devices from many locations on and off site. The ability to access and run productive operations remotely is much advanced. Recovery and restoration being completed in a timely manner should meet the needs of the business with IT as its central nervous system. Automatic and manual workarounds should be part of any response and recovery plan so that business can continue while the situation or failure is being addressed.

The evolution of programs to recover from failure or damage to technology as sketched in the previous sections lead to universal attributes of programs for business to respond and recover functions in general. We now look at what these programs should contain and ways to use them, starting with typical contents. In practice, a table of contents could be more detailed, to three of more levels instead of the two shown here.

- Business Unit Overview
  - Description
  - Business Owners
  - Structure, Staff and Location

- Scope of Program
    Scope
    Assumptions
    Exclusions
- Use of Program
    When to Execute the Plan
    Communicating
    Training and Testing
- Alternative Business Sites
    Other Business Sites
    Work from Home
- Business Critical Personnel
- Business Critical Assets and Processes
- Manual work Arounds

The framework shown supports a basic program, yours will be shaped to the industry or services delivered. Necessary data include at least lists of staff, assets, protocols, and key vendors for operating and assisting in resuming normal business operations.

Will it work in every case?
Now that we have our plans and detailed protocols (not shown because they are often long and differ across enterprises and locations), we ask will it work? Is our program a robust platform to assist in navigating FM and the business organization that it serves through an urgent situation, large or small, that could not have been closely predicted? Most, if not all, businesses answer “we need to test our plans”. Setting up scenarios or staging contrived crises is the standard for testing and drills. Testing should reflect a stress or removal of a key service or aspect of the business. In exercises, drills, and review, FM and other participants would follow the plan, communicating to assigned staff, executing initial workarounds, then reestablishing of services.

Up to this point, we have discussed the reasoning of disaster response and recovery, showing that plans follow a general structure, whereas detailed features can be particular to each organization, location, and circumstances. We outlined the evolution and use of plans, emphasizing the central place of technologies that link key business assets, processes, and vulnerabilities. We presented a general plan form.

Critically important at this point is to understand that plans to prepare for and recover from *disasters* can also be used with much smaller disruptive incidents, and the value of doing so. We do not have to wait for a natural disaster, fire, explosion, insurrection, plague, etc., or the requirement to review or exercise before pulling own the plan from the shelf and opening. We can and should utilize response and recovery plans as a resource for lesser events and more numerous incidents.

Objection
But isn’t it clumsy, wasteful, troublesome, and expensive to bring out a big plan for a small incident? No, not if we tailor the plan in advance to launch and follow through over a range of incident levels, beginning well below massive disaster. Doing so is doubly beneficial. (1) We have a developed means of dealing with any incident. We don’t have to invent as we go, just stay alert for opportunities to improve the plan. (2) At the same time, using our plans, even as configured for incidents of limited scale, keeps the plans familiar, maintained and ready for

use when required, whether for reviews, exercises, and drills, or actual emergencies - even large scale disaster or mayhem.

Illustration - water main break with no interior flooding

A few years ago, the author was FM at a major location with approximately 800 staff. A broken water riser (principal water main) affected numerous functions necessary for operations. Fortunately, there was no interior flooding. The fire suppression system was compromised, requiring immediate attention. Next, the author relates what happened.

> A water supply interruption sounds like a maintenance problem: just fix the pipe. Maybe a few departments would have to take the afternoon off, but everyone can be back at work tomorrow. Not quite, as was quickly shown in the ready, previously tested, plan. I contacted key stakeholders from the list in the plan, including vendors of services that we would require and other activities, such as deliveries, to delay. We established a fire watch that cost us a little sleep, but we knew just what to do. By the middle of the next day we had the fire suppression system back online and tested.
>
> I felt that the facility team did a good job and executed well. About a week later my manager's manager called and gave me somewhat of a scolding because the incident was just a broken pipe. Why the use of an emergency plan, bringing requirements for review, documentation, and reporting? I agreed that just assessing and repairing the break would be sufficient - as long as we did not have a fire. I was asked for a follow up report as required by the Crisis Management Plan. My report confirmed that this was not a large-scale disaster, just a broken pipe, but of critical importance to the facility and the business. Using the incident version of the disaster plan brought small additional expense beyond repairing the water main but helped ensure business continuity. We did not have to determine ad hoc how to respond. Identifying stakeholders, notifying the fire department and security, setting a watch… all were due and none missed. Our actions were already framed thoroughly. As we continuously assessed the developing situation, we were not at the same time formulating strategies, communications, and all else in the moment. That is, we could examine and interpret the particular problems and needs at hand, coordinating responses and recovery for best effectiveness, including considerations of cost.

Just fix the broken pipe? You decide.

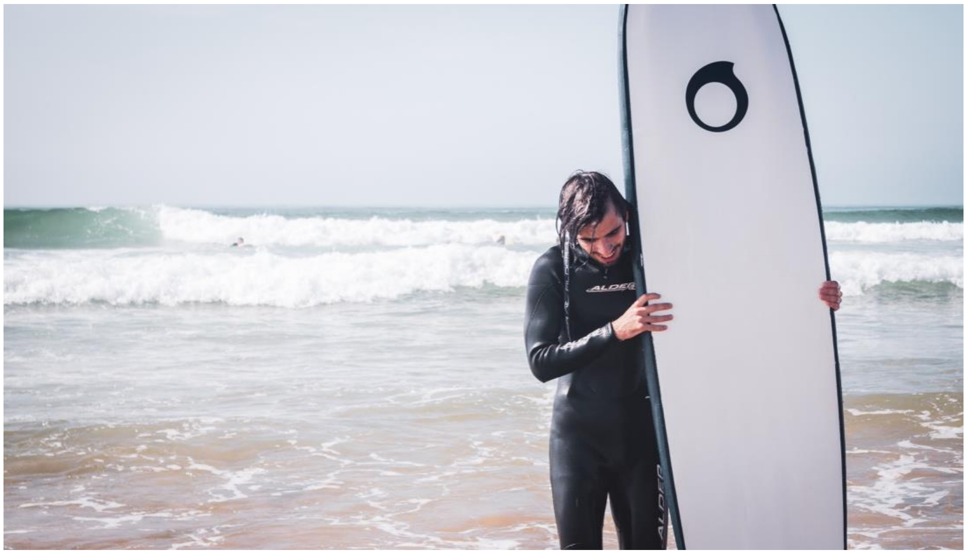

Photo by Oleksandr Kurchev on Upsplash

The author’s account continues.

> The lesson that I learned was that our plan, formulated and tested with answers to fit incidents of scope and duration smaller than disasters, was an efficient fit under the circumstances. Previously, the plan title had me focused on catastrophes: “A crisis is a CRISIS” and then there’s everything else. I now take a different view. The water main break, even though just an incident, was a failure in a key system. The solution played out much better using the Incident Management Plan (IMP) than could have happened without - especially the mitigation of additional risks that could be missed without the plan, or critical communications released smoothly and on-time to people in need of them. Parts of the IMP that were not used could have provided a clearer view into the failure, but failure circumstances were clear enough in this case. The IMP contained mechanisms to protect all the assets affected or at risk until the broken pipe as restored.
>
> An IMP can support most any emergency that may arise. By its exercise, staff are able to stay ahead of situations and not just react, communicating smoothly and making decisions. Much of what they would have to think up and initiate will already be in place, allowing them to deal with exceptional events and needs.

Conclusion

The adaptation and use of disaster preparedness and recovery programs and plans in incidents reduces but does not eliminate the need for stress tests as part of any FM disaster recovery and business continuity program. Usually, at least a few applicable incidents occur annually, contrasting with disasters, which of necessity must be rare. Benefits are that life and property protection, remedial actions, and communications at the time of an actual incident become sufficient, calm and predictable with competent use of a familiar IMP. When all of the parts of the IMP are complete in an actual incident, FM has a clear and organized basis to perform and improve each time. Use for incidents gets emergency response and recovery plans off the shelf and into familiar use. Take advantage of the opportunity.

(David Reynolds contributed editing.)