Supporting McCarthy's finding, Swiss Re said in a report to its shareholders that "total economic losses from natural catastrophes and man-made disasters amounted to USD $175 billion in 2016, almost twice the USD $94 billion seen in 2015."

Global insured losses from disasters also totaled $54 billion in 2016, up from $38 billion in 2015, according to Swiss Re, a leading reinsurance company.

Yet many organizations continue to struggle with their emergency and crisis management plans. This article includes some case studies that provide insights into common challenges during an emergency and recommendations on how organizations can respond and recover, quicker.

Lessons Learned

Recently, one of the authors was conducting a threat, vulnerability, and risk assessment for a large corporation on the East Coast of the United States. While at the corporation, the author met with the company's business continuity and emergency management director.

When asked about the company's emergency management program and response, the director produced a four-inch binder with a cover titled *Emergency Operation Plan (EOP)*.

For instance, everyone interviewed knew of the *EOP*, but no one knew their role or how to activate the plan should an emergency occur. They relied on the director to provide that direction.

When the plan was tested, one of the authors introduced a wildcard element by removing the director from the response process. This drastically increased the response time of the organization and taught a lesson that the plan did not account for: staff redundancy.

The organization needed a more granular version of its response so employees and key members of the crisis management team would know how to activate it should the director be unable to do so.

Communication. On August 23, 2011, in New York City shortly after 1:00 p.m. the high-rise building one of the authors was in began to sway. There was no communication about what was happening from building or security personnel.

A woman yelled out "it's happening again!" in a reference to 9/11, and people began to run to the stairwells to evacuate the building.

With the evacuation in full swing, an announcement was made: "A vibration has been felt in the building. Please stay at your location. More information will be provided."

Leadership. One of the authors had the opportunity to tour a critical infrastructure situational awareness room recently. The large facility was tiered like a movie theater, supporting floor-to-ceiling monitors that were concave to allow sightlines from within the room.

During a review of emergency operations, the author was assured that the response program was sophisticated and included redundancies in staffing technology.

"Has the building ever lost power?" the author asked, after which the room went dark. Emergency lights activated and everyone in the room began to look to others to take charge of the response.

Once time had elapsed, people gathered their thoughts, regained their composure, and transferred the critical systems to an off-site backup. The incident showcased the lesson that there will be a lapse in response time while people reference their crisis manual to find out who's in charge—creating overall recovery delays.

Changes. For every emergency plan the authors have tested, one of the key lessons is that an emergency action and crisis plan is a continual work in progress. As threats change, the plan must continue to adapt.

One example of this lesson in action occurred at a California hospital five

Applying fidelity testing to incident response training and execution can incorporate simple, but effective, gap analyses of critical program and process design qualities. This testing will help stakeholders understand their level of preparedness and response orchestration.

Validity. Check the validity of the original incident management plan. A review is the first step because the plan sets the framework for incident management and articulates all actions before, during, and after an incident—including training.

The plan should be based on a proven model, such as NIMS, and incorporate actionable, strategic, and tactical direction for each designated participant.

The organization should also look for gaps and assumptions made in the plan. For example, a specific role in the plan may be assigned to a functional leader but lack substantive direction for execution. Or, the designated leader may not have the right level of composure to execute his or her tasks under pressure.

If the plan needs to be updated to address these issues, the organization should make those changes before carrying out the full fidelity test. This is because the test will only work if the plan is comprehensive and actionable in terms of preparation, execution, and training requirements.

After re-testing, organizations should report on implemented improvements and their scale as part of established metrics, such as overall achievement of desired outcomes, reduction of time for task and process completion, and retention of information.

Training. Organizations should assess their current training by assessing the design, frequency, and knowledge retention of that training. It's important to determine whether existing training is actionable and produces desired outcomes from each participant with a minimum number of assumption gaps.

Good training programs will include a blend of interactive and practical content designed to be emotionally compelling for participants; interactive and practical exercises with the element of surprise; well-researched, relevant, and comprehensive training scenarios; and strict time parameters for completion of individual and team tasks.

Additionally, training programs should have metrics tied to gaps between demonstrated execution and desired outcomes, such as time to complete tasks and processes, as well as quality of task completion relative to desired outcomes.

Along with these characteristics, training programs should also include immediate post-exercise documented feedback with follow-up actions, and

This exercise will make it easier to uncover skill gaps. It is difficult for individual incident responders to objectively identify skill gaps on their own because of inherent psychological biases, such as confirmation bias, overconfidence, or timidity.

According to multiple psychological studies, humans learn better from the mistakes of others or when their mistakes are noted by friends and colleagues.

Identifying and mitigating skill gaps helps the entire incident management program and demonstrates the organization's commitment to improvement and resilience. When expressed statistically, the mitigation of skill gaps can help demonstrate the overall program's value.

Technology. Another benefit of well-designed and executed fidelity testing is the identification and mitigation of gaps in technologies used for incident management.

One of the most trivial—but often overlooked—issues is secure and interoperable radio communication. There have been numerous incidents, including 9/11, during which radio communication failed because of physical and electronic interference or other factors. Because radios were not interoperable, no one knew what others were doing.

interactive and practical content; continual program improvement; and meaningful metrics related to desired outcomes.

Incident management is best achieved through orchestration of individual components and responders and technology. Today, many organizations continue to struggle with achieving orchestration because of unaddressed skill gaps and assumptions in their planning. But this can be addressed and prevented in the future through fidelity testing.

"If you fail to plan, you are planning to fail," said Benjamin Franklin, and emergency and crisis management plans are no exception.

A well maintained and trained emergency management plan can provide significant dividends in recovery. Given the natural—and man-made—challenges ahead of us, emergency planning should be a staple in every organization.

Reasons for Failure

There are many reasons that emergency response plans fail. Below are some examples of problem statements that can contribute to failure.

Too much information. Emergency plans are not simple. And for large organizations, they can be lengthy and create information overload that increases the time it takes to respond to an incident.

Lack of training. Live action drills can be costly and create productivity challenges. Organizations have taken to Web-based learning, which exacerbates the problem because employees rush to get through the training, often retaining little of what they have learned. However, the organization obtains a mark for conveying the information and considers itself prepared.

Ilya Umanskiy, PSP, RAMCAP, MA, is founder and principal at Sphere State, Inc. Sean A. Ahrens, MA CPP, CSC, FSyl, is security market group leader for AEI/Affiliated Engineers, Inc., and specializes in threat assessment, crisis management, and security systems design. He can be reached at sahrens@aeieng.com.