

Strategies

for Effective Mitigation Planning



WALL STREET TECHNOLOGY ASSOCIATION™

TICKER
WWW.WSTA.ORG/PUBLICATIONS

By John C. Checco

No one knows more about mitigation strategies than a firefighter. Originally introduced in the late 1970s by the FAA as “Cockpit Resource Management” and later adopted by emergency services as part of their Incident Command System¹; Crisis Resource Management contains a trident for evaluating risks in any environment, known as the three *decision outcome avenues*:

- **Avoid:** Take measures to prevent a crisis.
- **Trap:** Identify and remedy problems prior to a potential crisis.
- **Mitigate:** Pre-plan remediation for high-probability or high-risk situations to reduce the negative effects of a crisis.

This article will discuss characteristics of mitigation strategies from the fire service as it applies to the enterprise.

Mitigation Goals

The most important prerequisite to any mitigation planning is to define the appropriate goals for the risks assessed by an organization. The weakest link in any mitigation planning is properly assessing risks and determining goals that meet the long-term business needs (rather than short-term stockholder and/or other political needs).

Firefighting itself is a mitigation process. The primary goal is not to put out fires, but to “protect lives and property.” Firefighters pre-plan almost every possible situation and outcome; and even have overlapping mitigation plans when the unexpected happens.

What can your organization learn about mitigation planning from 200 years of an organized fire protection service? Define the proper goals, define overlapping procedures to attain these goals, and always prepare how to handle the unexpected.

Compensating Controls

Compensating controls minimize minor disturbances and evenly distribute risk. The main features of compensating controls are a consistent

quality of service, high levels of automation, and minimal user intervention. Implementing compensating controls is necessary if a system requires uninterrupted use.

Examples include vehicle stability control, the steady-cam, uninterruptible power supplies, and even Federal Reserve Board interest rate adjustments.

Although the possibility of failure is greatly reduced, failures can be catastrophic. Mitigation for compensating controls requires the planning of large-scale remediation when a catastrophic failure occurs.

In continuing with the firefighting scenario, office buildings have fire-rated walls, specially designed stairwells and multiple exits. When a fire does occur (a catastrophic failure), the fire department is called as part of a mitigation plan.

Relief Valves

Relief valves, like compensating controls, constantly monitor minor variations in system activity; but relief valves use automation to aggregate multiple disturbances over time and create a frequent situation report to the end user. Relief valves have more variations in service levels and require more user intervention, but the customized monitoring and frequent adjustments actually increase the longevity of a system.

Water treatment plants, power grids and most other utilities all implement a relief valve strategy.

With relief valve strategies, the organization has precise control over how risks are mitigated, resulting in a low propensity for catastrophic failures. Mitigation planning for this process requires having access to appropriate resources and knowledge at any given time.

In addition to fire-rated structural components, an office building also has at least one relief valve

Strategies for Effective Mitigation Planning

strategy to mitigate the risk of fire. Sprinklers start mitigating problems early to prevent larger catastrophic failures.

Managed Security Service Providers (MSSPs)

There is a trend that the responsibility of information security is migrating from internal resources to outsourced providers. Although the transfer of responsibility may seem cost-effective, the mitigation strategy has fundamentally shifted from a relief valve strategy to a compensating control strategy.

Not only is there loss of control over smaller mitigation processes, but MSSPs utilize overall strategies that may not be appropriate to the mitigation goals of your organization. Organizations must ensure this paradigm shift still attains its mitigation goals.

Returning to our firefighting example, the fire department is considered a managed service provider. Although firefighters know how to save lives and minimize damage, they are rarely cognizant of which properties are considered more valuable to the client. And because of their internal organizational size and structure, fire departments will not dynamically change or implement untested strategies for a single client.

Using a service provider also introduces its own inherent risk of trust that requires its own mitigation plan². There are many examples where the outsourcing of business processes without the proper chain of trust and mitigation strategies has resulted in catastrophic failure; most recently the sub-prime mortgage crisis. Although it is unknown how this crisis could have been foreseen, there should have been mitigation strategies in place to minimize its effects.

No Single Solution

When does one use compensating controls versus relief valves? It really depends on the risk mitigation goals: compensating controls offer smooth operation with very few but significant stoppages, whereas relief valves require more interruptions but offer longevity.

Many organizations have a mix of remedial procedures that reflect several strategies; simply by deploying best practices that are characteristically different strategies without a clear set of mitigation goals. This has often led to gaps in procedures where remediation coverage was incomplete. Yet there is a synergy of implementing overlapping strategies if planned properly.

Although one strategy may work for a defined set of goals, the failure can occur when the goals are skewed. Black Monday was caused by the use of automated (compensating) controls spiraling out of control. The control strategy did not fail; the goal of creating a steady and uninterrupted nano-adjusting market was unrealistic. Today, NASDAQ employs relief valves to constantly monitor the market and suspend operations if key aggregators indicate an imminent control failure.

Some companies, such as factories dealing with hazardous materials, have very special fire mitigation needs. These organizations have internal fire protection staff as well as mitigation procedures created with surrounding fire departments. Both relief valve strategies (internally trained personnel) and compensating controls (fire department pre-planning) co-exist to provide the proper risk coverage.

Summary

The best security includes planning and applying all aspects of the Crisis Resource Management trident. Every strategy must strive towards attaining an explicit goal. If you only concentrate on where you see fire, you lose the entire building.

¹"Crew Resource Management," Dennis L. Rubin, *Firehouse Magazine*, July 2002.

²Recommended reading, "The Speed of Trust: The One Thing that Changes Everything" by Stephen R. Covey.

John C. Checco, CISSP, is an information security consultant and a NYS certified firefighter. He may be reached at Checco Services, 845-942-4246 or via email at john.checco@checco.com.