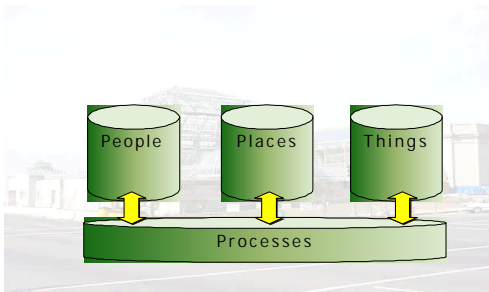


# CAFM, Terrorism and COntinuity of OPERations (COOP)

Eric Teicholz

There are dozens of ways that your business can be disrupted – from simple power outages to natural disasters. Over the years, most organizations have developed standard procedures and responses to respond to most disasters. The same is NOT true for terrorism. Criteria associated with business planning and emergency preparedness response are new and evolving rapidly. As yet, there are no standard operating procedures (responses) associated with terrorism that can be applied and implemented with facility management technology. This means that each organization must establish and build its own security and response model based on their perception of risk. However, as a result of the September 11 attacks, there is empiric evidence available about FM technology as it as its relates to terrorist-precipitated disasters.

## CAFM Technology



The data elements that make up COOP plans are pretty much the same components found in CAFM systems and include:

1. Organizational information about people – usually found in HR/ERP systems;
2. Place or locational information found in CAD and GIS systems;
3. Things or assets such as physical and IT infrastructure information are usually tracked by CAFM or other types of asset management systems.

### Some Definitions

1. **Disaster planning** deals with how technology can be used to model the potential impact of a disaster and how the organization can return to a steady state in the shortest possible time frame
2. **Business Resumption**: how technology can be used to support those activities associated with the plan - that is, how the organization repairs or rectifies disasters so that the it can function as intended
3. **COOP (Continuity of Operations)** is becoming the generally accepted term for business resumption or, more generally, for both planning and resumption functions. COOP is a business process that can be enabled by technology - a matter of setting priorities and strategy, establishing processes and measuring their effectiveness.
4. **Chief Security Officers** relate to people who have responsibility for creating and managing these plans. CSO's, at least in the private sector area, are often at the Senior VP level. The same way that a CIO is an established executive job – and has been around 15 years, CSOs probably will evolve in similar manner

COOP is made up of business process – and processes are best represented using workflow and collaboration automation tools that define processes containing the knowledge bases of an organization associated with disaster recovery and business resumption.

## COOP Technology Infrastructure:

There are four distinct components that lend themselves to, and best support, COOP planning and implementation:

1. The **Internet** which both enables data access to the disaster plan to anyone with a browser and the ability to store information off-site;
2. **Wireless communication** which enables automatic notification to the crisis management team and others in the form of e-mail, pagers, and telephone;
3. **Process and Document Management** tools enable workflow automation, status checking, escalation management, and remote/electronic document management;

4. **CAFM applications** which run the gamut of Building Automation (real time) systems such as energy, burglar alarms, fire; CAFM systems which have space, personnel and asset data; facility or condition assessment systems for critical building deficiencies and asset life cycle data; CMMS for help desk, work management and maintenance data; and real estate and property information for financial, occupancy, and lease data.

Most CAFM vendors are beginning to address issues raised by disaster planning and recovery. At the most basic level, vendors might offer templates, forms and check lists for planning, security procedures, insurance, or other generic COOP functions. Some have specific help desk functionality for emergency preparedness. Some current versions of CAFM software support very flexible workflow for diagramming business processes with on-the-fly process modification and escalation. Some products will integrate with external real-time systems such as fire and burglar alarms. Some link to internal or external groups such as FEMA, the weather service or the Red Cross and some create logs of actions taken so that processes and procedures can be audited, benchmarked and improved. Each vendor is different, but most at least are beginning to address some aspect of the problem.

### **COOP Planning Process:**

COOP planning consists of 3 stages: planning, response and recovery. As mentioned, criteria for planning/response is evolving and there are unfortunately no technology standards that can be applied to facility/infrastructure management as it applies to terrorism.

#### 1. Planning

Planning is made up of a number of tasks such as figuring what, when, why, where and how decisions will be made and actions taken both internally and externally with relevant clients, customers, employees, and local, state and federal agencies. Tasks might include:

- Audits (e.g., insurance, base line information)
- Entering/classifying crises
- Risk assessment
- Establish response policies
- Selection of management and response teams
- Establishment of alerts and notifications
- Determination of tasks with various stake holders

Typical CAFM data to support these tasks include:

- Employee/asset locations
- Means of egress
- Evacuation plans
- Contact information
- Facility condition assessment Data
- Utilitizes/telecom data
- Fire protection/security plans
- Hazardous material plans

#### 2. Response

Response relates to the plan's execution in order to maximize life safety issues and protect property. It seeks to accomplish this with minimal financial loss and business disruption. Specific tasks might include:

- Plan deployment and communication
- Establishment of off-site command and control center
- Communication of information between crisis team and other groups
- Accessing and modifying scenario based on data
- Document everything (damage to facilities/harm to people) before/after crisis

Again the specific crisis will probably not be modeled precisely so real time workflow modification becomes a powerful programming tool. The primary technology requirements during this stage relate to process modification, communication (automatic if possible using wireless devices and the Internet), Help desk/work management software.

### 3. Recovery

The goal of recovery or resumption is to resume normal operations in the shortest possible time frame – again with minimal personnel injuries, damage, liability and financial loss. Primary tasks associated with the reestablishment of this equilibrium within an organization are the documentation of the damage done, the generation of benchmark data, the updating of relevant planning and training data and the evaluation of stakeholder performance and procedures. There is a great deal of FM technology to support these functions such as space planning (including stacking and blocking), facility conditions assessment, before/after asset comparisons, move planning and business process modification.

### **COOP – Lessons Learned**

Not every disaster can be predicted but, with sufficient scenario planning, most likely terrorist and natural disasters can be planned for. For each scenario, key facility related data is required along with business processes automation. The more automated the process and communication links, the more likely it is to be executed rapidly and correctly.

Several requirements related to FM technology became clear after the events of 9/11:

Strong Management Commitment – to disaster planning/business recovery.

Clearly Defined Processes – The documentation and testing of precise, prioritized incident/emergency management processes, trained crisis management teams and response preparation and testing.

Mass Notification Procedures- Having information on alerting and notifying both management and employees of status and situation. 800 numbers for staff to call, radio broadcasts, and even pre-setup alert websites.

Groups/ Department Critical Needs Charts- Detailed information, usually residing in the Rooms or Personnel tables of CAFM systems, that identify the mission critical people and what their IT, telecom and asset needs are in an emergency.

Information on available crisis spaces- Current and relevant FM databases and IT technology to support COOP including, for example, conference rooms with extra network/telecom capacity for use as command centers (if they are internally located), rally points (where crisis team or other groups might go in case their spaces are unavailable) or for temporary work areas for displaced personnel.

The importance of using the space planning modules for use in planning sessions. This relates to coming up with possible disaster scenarios using CAFM stacking/blocking software to query, for example, the number of mission critical employees that might be affected and then determining the cost to provide these individuals with dedicated hot site locations or comparable spaces outfitted in another building.

### About the Author:

Eric Teicholz is president of Graphic Systems, Inc., a Cambridge-MA, independent FM/RE technology consulting company. He can be reached at [teicholz@graphicsystems.biz](mailto:teicholz@graphicsystems.biz), 617 492-1148x106 (tel) or through the company's website: [www.graphicsystems.biz](http://www.graphicsystems.biz)