

White Paper: Incident Management

By Michael Miora, CISSP

President & CEO
ContingenZ Corporation
mmiora@contingenz.com

April 20, 2002

Table of Contents

| | |
|--|----------|
| Introduction to Incident Management..... | 2 |
| Incident Response & Crisis Handling | 4 |
| Continuation & Recovery Planning..... | 6 |
| Conclusion | 7 |

ContingenZ
CorporationTM

Training ▪ Education ▪ Consulting

ContingenZ Corporation
227 Fowling Street, Playa del Rey, CA 90293
www.contingenz.com ▪ info@contingenz.com
310 306 0111 ▪ 310 306 1612 fax

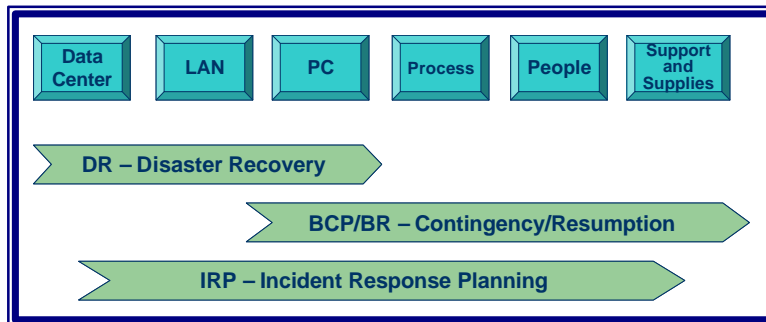
Incident Management: Recognize, React, Respond

INTRODUCTION TO INCIDENT MANAGEMENT

What is Incident Management

Incident Management is the process of recognizing events that will affect the business, reacting appropriately to those events, and then responding to quickly resume normal corporate operations. Events can range from public relations missteps, internal or external security breaches, natural or unnatural disasters, terrorism, unintended privacy violations, unexpected financial situations and a host of other conditions that interrupt normal business activities.

Recognize, react and respond to continue the corporate mission.



The Incident Management process transcends the conventional thinking that pigeonholes problems and solutions according to their cause. Instead, it focuses on the enterprise need to function well in the face of adversity regardless of the cause. When planning is enterprise-wide and cross discipline, then there is Incident Management.

What Makes Incident Management Different

Incident Management takes an enterprise-wide, cross discipline view of an enterprise and its business objectives so that all work done to counter any threat can be made directly applicable to all other threats. For example, a terrorist attack on a building with a resulting outage in information systems may have much in common with a natural disaster such as a flood or a local issue such as a power failure. The measures taken to counter that threat can also act to counter the threat of internal sabotage by disgruntled employees.

A long and wide view to enhance effectiveness and reduce cost.

Incident Management takes a long and wide view to bring together the disparate elements of Incident Response, Crisis Management, Disaster Recovery Planning, Business Continuation Planning, Health and Safety Plans and other such projects into one overriding project that enhances protection with increased cost-effectiveness and a better Return on Investment (ROI).

Who is Responsible for Incident Management

The conventional wisdom has been to assign responsibility for incident management based on the cause and the potential impact. Therefore, natural disasters were within the domain of risk management while security breaches were assigned to the technologists in the Information Security department, and the legal department handled privacy breaches. This conventional wisdom increased the cost of Incident Management and prevented optimal utilization of existing corporate resources and capabilities.

con-TIN-gen-ZEE: A company that improves incident management posture by increasing effectiveness and ROI using an enterprise-wide, unified methodology.



Today's connected, global and distributed enterprises have recognized that all incidents share the same need for recognition, reaction and response. Therefore, they have lowered costs and increased effectiveness by including all incidents within a single overarching Incident Management methodology. While responsibilities for specific actions, including detailed plans and test routines still fall to the appropriate department, the overall process and plan benefits from sharing corporate resources.

Incident Management responsibility is shared across the enterprise.

Why Incident Management

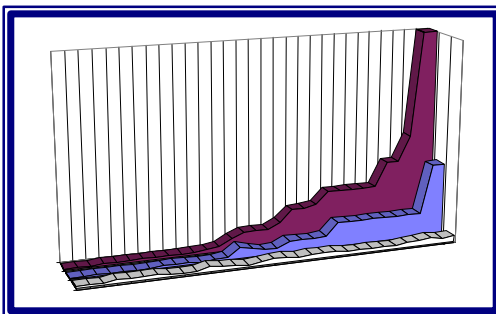
It is almost a certainty: Every major company will face a significant incident within three years. A global Incident Management methodology will lessen the affect of that incident on the corporate brand, image and revenues. No longer do we look at incidents as earthquakes or tornados, hackers or corporate espionage, terrorism or sabotage. Today, an incident can be any one or more of these, or can be something as simple as an accounting error that requires rebuilding and reestablishing financial baselines. It can be something as important as a breach of privacy that reveals private information about corporate customers.

Any incident can cause corporate harm; every incident is less harmful if you see it coming.

Any incident can cause corporate harm; every incident is less harmful if you see it coming. Incident Management is about getting prepared so that you can see an event coming, mitigate the harm beforehand, and respond quickly and effectively so you can get on with business.

Incident Management and ROI

Calculating the return on investment (ROI) for conventional Disaster Recovery or Business Contingency Plans was difficult because it relied in probabilities of events occurring and likelihood of impact on operations. These small probabilities were not conducive to persuasive presentation or analysis.



Incident Management does not rely on probabilities because the set of events encompassed by Incident Management occur with regularity and predictability.

Incident Management does not rely on low probability events for calculating ROI.

Incident Management includes not just disasters, but normal business occurrences that must be handled on a regular basis.

Events included within Incident Management include normal business migrations as well as system outages. They include security or privacy breaches caused by normal errors as well as those brought on by hacker attacks.

INCIDENT RESPONSE & CRISIS HANDLING

Introduction and Objectives

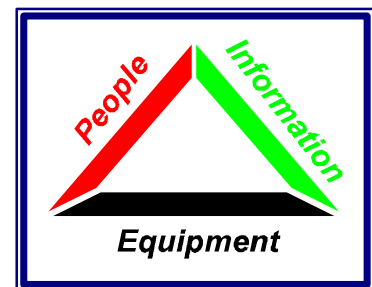
Every enterprise must be prepared to confront an incident that threatens, may threaten or has threatened security, privacy or the general operations of the company or its customers. Incident Response and Crisis Handling is the area of expertise and specialty that puts in place the processes required to prevent an incident from becoming a crisis; an Incident Response Team (IRT) is the active operational element that handles incidents. An IRT provides the enterprise with a measurable return on its investment.

Prevent an incident from becoming a crisis.

An IRT is a multifaceted, multitalented group of individuals specially trained and equipped to recognize incidents, react to them appropriately and respond quickly and effectively – they provide the first reaction to an incident. Their immediate goal is to take control of a situation in order to contain the scope of a potential compromise, to conduct damage control, and to prevent the possible spread of a compromise to prevent or reduce loss.

Take control to reduce compromise and loss.

The teams respond to emergencies or incidents. Such incidents might be characterized as any unwanted or, in some cases, unexplained behavior. An incident does not always indicate something unwanted; it also can be something that is merely unexplained or out of the ordinary. Response acts not only to defend or prevent further damage, but also to discover more information or to verify facts – in essence, it is part investigation and part education.



Recognize ▪ React Respond

If locks, checks and balances, and other preventive measures were foolproof, incident response would be unnecessary. Banks put huge vault doors, time locks, and other seemingly impenetrable defenses into their buildings, but they recognize that these measures cannot be 100% effective. Consequently, they also install alarm systems. Alarm systems detect when one of the defensive barriers has been breached, but that knowledge is of little value if no one hears the alarm or, if having heard the alarm, there is no clear response.

An alarm is not useful if nobody hears it.

Building the Incident Response Team

Establishing an Incident Response Team is a complex process that must be given careful thought and be based on comprehensive planning that encompasses all three major risk mitigation areas: People, Information and Equipment. Moreover, the IRT should be built with an enterprise-wide, cross-discipline perspective. Specifically, the IRT must be built in coordination with the functions of Contingency & Continuation

An Incident Management, team handles all three risk mitigation areas.

Planning and with Disaster Recovery Planning. When all three of these response and protection capabilities are developed together then true Incident Management takes flight.

The overarching goal of responding to an incident should always be to prevent further damage and to restore functions to normal as expeditiously as possible, consistent with organizational policies. A clear, written mission and charter establishing the team is essential to achieving this goal as well as to the clear presentation of ROI. The mission and charter should establish why the team exists and what the organization expects from the team. Without a clear definition of mission and an idea of what can be expected from the team, internal cooperation and support for the team will be difficult to obtain and even more difficult to sustain.

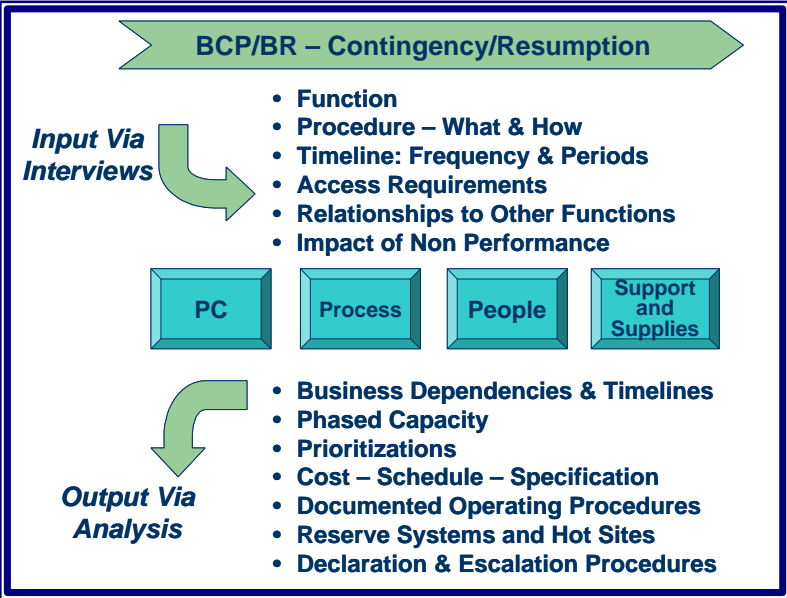
The overarching goal is to minimize damage and to restore functions quickly.

The makeup of the team has everything to do with how effective and responsive it will be in an emergency. Careful selection of team members at the outset will provide for an effective, cohesive group with the right skills, authority, and knowledge to properly deal with a range of known and unknown incidents.

While technical ability is essential to an effective team, this should not be the overriding characteristic. Exceptional communications skills are critical because, in an emergency, quick and accurate communications internally and externally are necessary. Inaccurate communications can cause the emergency to appear more serious than it is and therefore escalate a minor event into a crisis.

Good communication is as important as technical knowledge.

CONTINUATION & RECOVERY PLANNING



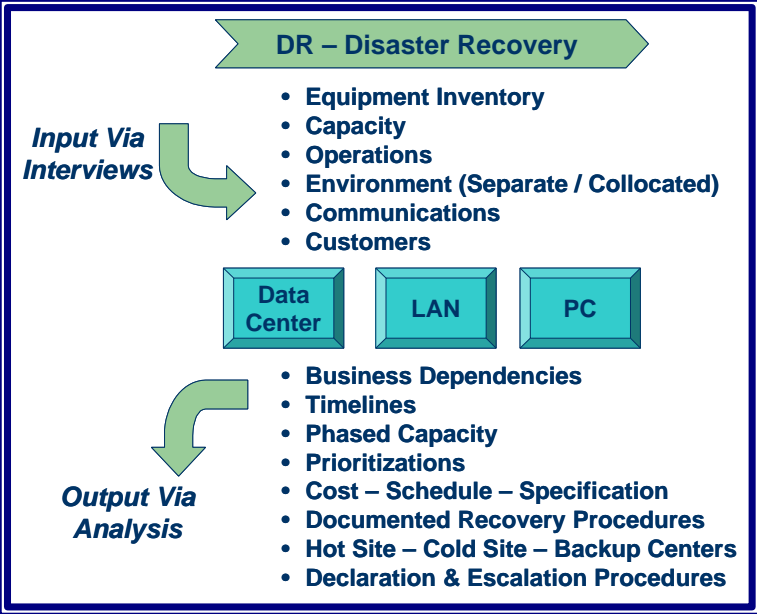
Continuation and Recovery planning problems are serious – the solutions are hard. The purpose of a Continuation and Recovery planning project is to protect the enterprise, including its people, equipment and information, by planning the recovery of company assets in the event of natural or unnatural disasters.

A key element of minimizing the risk at the lowest possible cost is recognizing that there are a variety of risks whose effects are similar in nature even when the cause may be very different.

A Continuation and Recovery planning project accomplishes three goals. First, it determines where true risk exists, defines the impacts of the risk on business operations, and develops strategies for minimizing exposure to risks.

Second, the project defines the activities required to implement the strategies and to acquire the services to support those activities.

Third, it develops and tests a detailed set of policies, procedures and practices to provide for recognizing when a threat has impinged on the enterprise, reacting effectively and quickly to mobilize resources, and responding to the damaged caused by the threat to restore full operations. It is important to note that the recovery steps are independent of the specific threat.



CONCLUSION

Enterprise Incident Management is the natural evolution and unification of the techniques, methodologies and technologies used over the past 20 years. Incident Management empowers experts from a variety of disciplines to work together to solve problems; information security, law, risk management, business continuity, public relations, audit, finance and other disciplines represented in the enterprise can now join forces in a coordinated, disciplined manner so that budgets can be justified well and progress can be made quickly.

The disaster recovery and contingency planners of the past had to fight for budget using scare tactics and pointing to rare events. The Incident Management and Response planners can now make simple, concise and compelling business cases for proceeding apace with the planning efforts.