

White Paper: Building an Incident Response Team (IRT)

By **Michael Miora, CISSP**

President & CEO
ContingenZ Corporation
mmiora@contingenz.com

November 14, 2002

Table of Contents

Incident Management Overview	2
An Overview of the Incident Response Team (IRT).....	4
The IRT	6
The Team Planning Process.....	8
The Response Profile – The Steps of the Process.....	11
Special Considerations	14
Post Response Profile.....	17

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

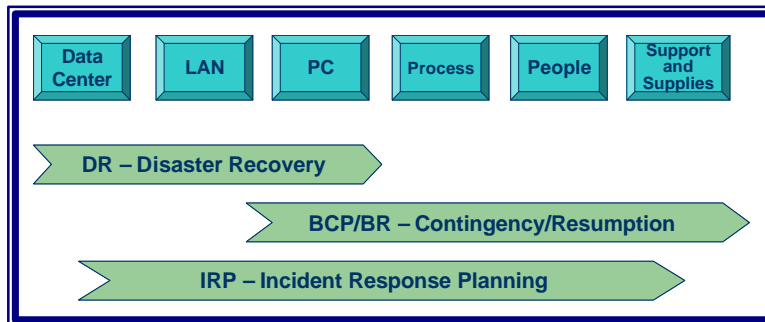
Incident Management: Recognize, React, Respond

INCIDENT MANAGEMENT OVERVIEW

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.

Incident Management Approach

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).

Incident Management Responsibility

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

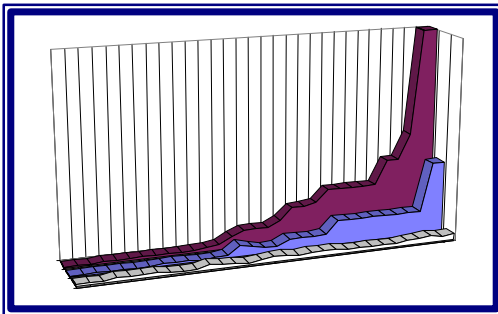
It is almost a certainty: Every major company will face a significant incident within three years. A global Incident Management methodology will lessen the affect of that incident on the corporate brand, image and revenues. No longer do we look at incidents as earthquakes or tornados, hackers or corporate 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.

AN OVERVIEW OF THE INCIDENT RESPONSE TEAM (IRT)

Objectives

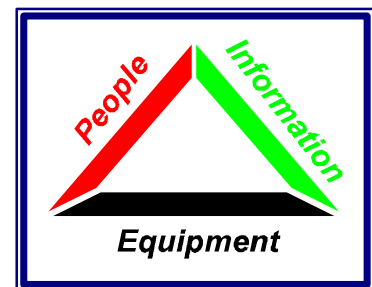
Every enterprise must be prepared to confront an incident that threatens, may threaten or has threatened security, privacy or the general operations of the company or its customers. Incident Response is the area of expertise and specialty that puts in place the processes required to prevent an incident 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.

The IRT handles and coordinates all incidents.

An IRT provides 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. The IRT is charged with taking control and bringing in corporate resources and elements as required to recover and resolve the emergency situation.

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.



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. The IRT is charged with listening for the alarm and reacting to it appropriately.

An alarm is not useful if nobody hears it – the IRT is charged with listening for the alarm and responding appropriately.

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 Planning and with Disaster Recovery Planning. When all three of these response

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

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.

Composition

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. It is the IRT that must have at its disposal the proper business, technical, management, financial and legal knowledge to hear the alarm, recognize the issue, react with a pre-planned action plan, and respond to the incident-in-progress.

**Recognize • React
Respond**

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.

THE IRT

Team Composition

An Incident Response Team (IRT) can provide organizations with a measurable return on their investment in computer and non-computer security and assurance mechanisms and intrusion detection systems. The primary value of an IRT to an organization is in reducing the impacts and the cost of the incident. Intrusion and other detection systems can indicate that something occurred; when an incident occurs, the intrusion detection system makes us aware of the incident. We make use of this knowledge by responding to the situation appropriately; the IRT is the mechanism for doing something about that occurrence.

An IRT provides a measurable ROI.

The IRT is a multifaceted, multitalented group of individuals who are specially trained and equipped to respond quickly and effectively to computer emergencies. IRTs come in a variety of forms and compositions. Some teams are static, established groups; others are assembled dynamically to fit a specific mission or to deal with specific emergencies. Often the most effective teams are characterized as a mixture of these two approaches.

These "hybrid" teams generally have a standing core membership comprised of both technical and non-technical members. When a situation arises that must be addressed by the IRT, additional members with specific skills are added to meet the requirements of handling the incident in progress. Once the incident is resolved, the team reverts to its core membership status.

The Overall Mission

The IRT provides the first reaction to an incident. The team's 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 or reduce loss by limiting the possible spread of a compromise if possible.

Maintaining a dedicated IRT at the ready, 7 days and 24 hours, is a costly and unjustifiable proposition. Virtually any organization today, no matter its mission, will be hard pressed to justify funding a team whose members have no other responsibilities. The cost fiscally as well as in lost resources of maintaining a team of highly trained resources, with only emergency response roles, is untenable and unjustifiable. In today's dynamic corporate environments, the team members who are activated for emergency response during active incidents also have important and ongoing roles in the corporate environment.

Take control to contain the incident in order to minimize the loss and damage it causes.

These roles represent the full spectrum of corporate functions required to fulfill the incident response functions. Therefore, team members will be experts in areas ranging from marketing to manufacturing, security, risk, human resources, accounting, legal, press relations and all other key corporate governance and operational areas.

Often, response teams provide and maintain training and awareness programs for the organization. These awareness programs benefit an organization by pointing out risks and ways to avoid them. In addition, delivering awareness programs makes the team members more visible. As a result, employees are more likely to notice and report potential incidents since they are trained to be aware of some of the symptoms of incidents.

Some History

In November 1988, the infamous Internet Worm was unleashed, and it wreaked havoc by disabling a significant portion of the Internet. As organizations attempted to deal with the worm, it quickly became apparent that a coordinated response to such incidents would have helped to lessen the impact and to significantly speed recovery.

There were two significant problems during this attack. First, there was no central repository to which to report information about the attack or from which to gather information that might be useful to speed containment or recovery. Second, few organizations were prepared with teams standing at the ready to respond to the attack. The result of these two issues was that the response time was slow and uneven, and each organization was forced to develop its own countermeasures with only occasional, informal support from other attacked entities.

Dealing with incidents that cause loss requires an Incident Response Capability and its core element, the IRT.

The most common response at that time was to disconnect from the Internet until the issue was resolved, but that solution is not possible or reasonable 15 years later. Moreover, the issues of systems outages are now inextricably intertwined with incidents that involve computers and systems only peripherally or even not at all. For example, some incidents may leave systems intact yet prevent employees from entering the company premises.

Therefore, today's mainstream organizations must be prepared to deal with the myriad of incidents that can cause damage to systems or reputation and cause loss to revenues, stock prices and public confidence. This preparation most often takes the form of an Incident Response Capability and its core element, the Incident Response Team (IRT).

THE TEAM PLANNING PROCESS

Establishing an IRT is a complex process that must be based on comprehensive planning. Before establishing an IRT, the organization needs to specify the IRT scope, the response requirements and the basis for these requirements. The organization can then decide on specific goals for the team and then start developing the overall guidelines for the team. The team charter, composition, and detailed planning will flow from these requirements and guidelines.

The Team Charter

A clear, written mission and charter establishing the IRT is essential for success. This document establishes why the team exists and what the organization expects from the team. This document also summarizes the reasons for establishing the incident response capability.

A clear and written mission and charter establishing the IRT is essential for its success.

The IRT mission and charter should be based on organizational philosophy, policies and practices. These include information security policies, privacy policies, corporate mission statement, performance practices, financial policies and practices, corporate bylaws and governance rules, legal and regulatory requirements and others. If some of the IRT governing policies are not yet written, then it becomes important to suggest them during the team planning process.

Establishing a team without having appropriate policies in place can at the least put the team at odds with its own organization. Worse, without the authority provided by executive policies, the team may be unable to function effectively during a crisis and may even be considered an adversary by other parts of the organization that have not been affected by the incident in progress.

In any case, regardless of how the policies are built, there must be an unambiguous sense among the IRT that those responsible for taking actions in good faith will not suffer reprisals as a result of taking those actions. For example, based on facts in evidence at one time or another, a member of the team might decide to disconnect an operational system from the Internet because it appears to be under attack or to have been compromised. Should this turn out to be a false alarm of some sort, the individual authorizing the action should suffer no reprisal or sanction by taking what he or she believed was a legitimate action to stop or to respond to an attack.

There must be a clear understanding that taking actions in good faith will not result in reprisals in case those actions are unpopular or even erroneous.

Interactions

The IRT may need to interact with a variety of organizations inside the company, with government agencies, with private and public incident response organizations, and with vendors and customers. These possible interactions depend upon the company and its organizational structure, industry, regulatory status, and overall philosophies. The range of interactions should be specified in

the IRT procedures and practices, including guidelines and approval processes as required.

Internal Interactions

- Management
- Marketing and Sales
- Human Resources
- Legal Department
- Consumer Relations
- Investor Relations
- Public Relations
- Technology
- Compliance Committee
- Audit and Risk Management
- Business units

External

- Service Providers and Consultants, including those used regularly to augment technical skills and knowledge as well as incident handling experts.
- Vendors
- Law enforcement
- Utilities
- Internet service providers
- Other incident response teams in similar and diverse industries and sectors

Establishing and Maintaining Baselines

In order to be able to effectively spot that which is out of the ordinary, the IRT must define normal. This is especially true for security and privacy incidents, but is also applicable for product issues, regulatory investigations and others. False incidents occur when the team does not have adequate knowledge of a normal profile and, hence, interprets a normal activity as abnormal.

A set of well-established baselines are essential for the determination of whether an incident is real or a previously not noticed normal condition.

The IRT planning process must therefore include establishing baselines for normal operations and designing procedures and practices for maintaining that baseline over time so that when an incident occurs, the baseline is still accurate.

Selecting and Building The Team

An effective IRT is comprised of the following elements, dictated by the incident at hand:

- People
- Skills
- Knowledge
- Equipment
- Access
- Authority

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.

The first inclination, frequently, is to select the most technically knowledgeable individuals available as members of the team. While technical ability is essential to an IRT, this should not be the overriding characteristic. Given aptitude and motivation, appropriate technical skills can be learned. Indeed, during the course of an incident handling situation, an adept handler can draw on the technical expertise of people, either internal or outside, to augment his or her skills and knowledge.

Technical expertise is essential but other skills are required for an IRT to succeed.

Maturity and the ability to work long hours under extreme stress and intense pressure are crucial characteristics. Integrity in the response team members must be absolute, since these people will have access and authority exceeding that given them in normal operations.

Exceptional communications skills are required because, in an emergency, quick and accurate communications are needed. Inaccurate communications can cause the emergency to appear more serious than it is and therefore escalate a minor event into a crisis.

THE RESPONSE PROFILE – THE STEPS OF THE PROCESS

While a complete treatment of incident response procedures is beyond the scope of this paper, some general response steps and considerations are applicable to all incident-handling teams and are summarized here.

Step 1: Observe and Evaluate

A response team leader must assess the situation as quickly as possible, based on available information. The leader should make a preliminary estimate of the type of incident, its scope, the people involved, the data or systems affected, and then begin formulating first responses based on pre-existing procedures and action plans.

Quick evaluation and call to action is essential.

This is the point at which the team leader or other responsible person orders a move from a state of standby monitoring to one of active monitoring, focused on the particular event or events. It is important to maintain standby and baseline monitoring activities during an actual incident because the obvious event might well be a ruse designed to divert attention from a more serious attack.

If proper planning has taken place, the team leader usually will be able to direct a specific course of action in response to a particular incident. The leader can choose from a menu of planned responses while drawing on only those resources necessary to execute that particular response. Doing this minimizes the impact on staff at all levels and allows the incident to be dealt with efficiently and effectively. However, the more unique or complex the situation, the more likely it is that a complete team response may be required.

Step 2: Begin Notification

Once the team leader establishes that an incident is in fact in progress, notification must begin to appropriate individuals within the organization, consistent with the type of situation. Notification and timing should be carried out, whenever possible, according to existing plans.

In most cases, the IRT leader will be able to identify the incident as one calling for a prearranged response. The leader, having the authority and confidence to carry out such a pre-approved response, will notify those appropriate to the incident and carry out the contemplated actions. In other cases, the situation might not be so clear, and the notification process might include additional personnel with authority to decide on various courses of action.

In most cases, the IRT leader will be able to identify the incident as one calling for a prearranged response.

Step 3: Set Up Communications

Team members, especially when dealing with remote or multiple sites, must be able to communicate easily and securely with one another as well as with management representatives. Team members need to be able to communicate data, status updates, actions, responses, and similar events. Communications

should flow securely to the designated IRT leader for coordination. The team leader must be able to direct and advise other team members, but the potentially sensitive nature of an incident may require that these communications be handled out of band and through secure means.

Step 4: Contain

The IRT's next course of action is to contain the incident. The goal is to limit the scope of any compromise as much as possible. Whereas containment may involve steps such as disconnecting systems from the Internet, doing so might limit the organization's ability to catch an intruder who is currently active on the system. The priority level assigned to intruder identification and prosecution is a part of the mission and charter of the team, modified by the specific action plans in use for a particular incident.

The containment versus capture decision is usually made prior to the incident.

Step 5: Identify.

Once the team has taken steps to contain the incident as much as possible based on the specific circumstances, it should focus on identifying exactly what happened, why it happened, how it happened, and then identifying steps that can be taken to prevent a recurrence. This effort also might involve identifying who, if anyone, was or still is involved in the incident or attack.

Step 6: Record

All IRTs should be trained to document everything during an incident. No event or detail is too small to record when responding to computer emergencies. Always try to answer "Who? What? Where? How? When? Why?" This is especially true when dealing with criminal activity when there is an expectation that the intruder will be prosecuted. Keeping accurate records of what happened and the team's actions can prove pivotal in the organization's ability to positively identify the cause or source of an incident and prevent similar incidents in the future. It is also essential to record costs as they are often subject to recapture through insurance policies, but only if well documented in real time.

Real time record keeping is essential for post-event evaluation and insurance reimbursement.

Step 7: Return to Operations

For most business managers and executives, restoring operations is of paramount importance. Frequently they will pressure the IRT to put off all other activities and to direct all resources to that end. Except in extreme cases, that pressure should be resisted, and the orderly carrying out of all preceding steps must be assured. As soon as possible, the IRT should assist operations personnel with bringing capabilities and systems back online and returning them to full operating capacity. In some cases, hard drives, logs, and even entire systems may need to remain off-line until detailed forensics examinations may be completed. In these situations, backup systems should be used to bring systems and operating capabilities back online.

Step 8: Document and Review

While all IRT members should keep careful notes and records at all times, it is important to note that formal procedures to document incidents and resulting actions is vital to the overall success of the incident response effort. This documentation can form the basis for new approaches, procedures, policies, awareness programs, and similar changes. Documenting successes and failures can provide the organization with a realistic view of its security posture and of its capability to respond to emergencies, and in some cases can justify the expenditure of additional funds on training or technology.

SPECIAL CONSIDERATIONS

Involving Law Enforcement

The decision about whether and when to involve law enforcement in an incident response is one that must be carefully considered during the planning stages before an incident takes place and then evaluated continually during an event. While most organizations recognize the benefit of a close relationship with law enforcement, involving such agencies when responding to a computer emergency can have consequences beyond those that are immediately evident.

Involving law enforcement has implications the obvious.

Clearly, local and national law enforcement agencies have a great deal to offer when establishing IRTs and developing incident handling capabilities. Many law enforcement agencies have specialized units dedicated to computer crimes and issues. These can be valuable resources, likely to have a wealth of threat and resolution data on hand. For this reason, it is important to partner with appropriate agencies to take advantage of their experience and to establish relationships. Knowing whom to contact in an emergency not only will save time and frustration but may mean the difference between on the one hand, repelling an attack on the one hand catching and successfully prosecuting the perpetrator, which may help prevent future attacks.

Obviously, local laws and statutes may dictate specific notification requirements that an organization is obliged to follow in the event an actual or suspected incident occurs. Careful review of local laws, statutes, and ordinances should be undertaken to ensure the organization complies with notification requirements and other legal requirements.

Laws and regulations may dictate notification requirements.

When there is a choice to be made, the organization must weigh carefully the decision to involve law enforcement and especially the timing of doing so. In most cases, formally involving law enforcement means that the organization may have to turn control of the incident and subsequent investigation over to the agency whose jurisdiction it is to investigate the crime.

While most professional law enforcement agencies will work with an organization to minimize any adverse impact on normal operations, this may not always be feasible. Because the goals of law enforcement often are different from those of others, especially in the case of commercial enterprises, law enforcement may not always consider the business or operational impact of response on the organization under attack.

The goals of law enforcement are different from those of industry.

Since law enforcement's mission is to investigate criminal activity, its focus will naturally be on identifying, tracking, and locating the intruder. This can, in some cases, result in seizure and removal for forensic purposes of systems and data, even systems that may be critical to the continued operation of the organi-

zation. In the case of a business, this might well mean loss of necessary servers or workstations while an investigation is under way, with a possibly devastating effect.

Indeed, decisions about a preferred response may be taken out of the hands of managers and executives when law enforcement enters into an incident response situation. A commercial business might focus on identifying the vulnerability that made the attack possible, protecting against that vulnerability, and restoring systems to full operating capability. If, during the course of these efforts, the perpetrator can be identified, law enforcement will be informed, but such identification is rarely the overriding objective.

On the other hand, when law enforcement is involved, identification and prosecution of the perpetrator is the primary objective. Establishing contact with appropriate law enforcement agencies before the organization is forced to respond to an incident will help the IRT plan when to notify law enforcement and how most effectively to align both sets of objectives when dealing with an incident.

Law enforcement is quickly realizing that organizations are reporting incidents sparsely. As far back as the 1980s, organizations such as the FBI, CIA and NSA realized that only a small percentage of incidents were reported to the government. Companies' fear of publicity and other impacts prevented their going public with breaches and other types of incidents. To counter this long-standing trend, in late 2002 federal law enforcement officials have begun a campaign to bring their activities into alignment with the needs of the commercial sector. The hope is that this change will encourage companies to report incidents more frequently and more quickly.

Law enforcement is aligning their activities with those of the commercial sector to encourage greater incident reporting.

Need to Know

Protecting information about an incident in progress is essential, not only to a successful response but because it can have serious and long-term legal, privacy, security and other ramifications as well. Those charged with handling an incident must use out-of-band communications, such as cellular telephones, pagers, and encrypted electronic mail systems not connected to the system under attack to ensure that knowledge of the incident is restricted to those with a need to know. Attackers could intercept team communications, if passed through in-band or normal channels, and use that information to "cover their tracks" or even to prolong an incident.

Out of band communications are essential for real time incident related communications.

Responding to incidents always involves gathering information about systems, users, activities, and events. In most cases, sensitive system and even personal information may be collected. Members of the team frequently make assumptions about the identities of those responsible for the incident, during the

course of their response and investigation. These assumptions are based on interim data that is continually collected, refined and modified during the course of an emergency response. It is critical that this information remain confidential. And so it is therefore essential that the IRT disseminate information about the incident on a strict need-to-know basis using secure communications channels. Limiting knowledge about an incident and securing it against security breaches will help ensure that sensitive information remains in the hands of those who need it to perform their duties.

Management Role

Management plays a key role in the formation, operation, and support of an IRT. Ideally teams should be composed not only of technical personnel but of managers with sufficient authority to assist the team in taking actions that contain an incident and protect data and systems from further compromise. Management support for planning, establishing and enforcing policies, and for pre-authorizing responses is essential. Management support of the IRT is critical since without solid backing from the highest levels of management, the IRT will be frustrated in its attempts to carry out its mission.

Public Affairs

The nature of interconnected systems today all but guarantees that any incident will become obvious to partners, customers, clients, and others. In many cases, the organization will be compelled to advise its constituents continuously of the status of any outage or degradation of services resulting from an incident and the reasons behind it. Therefore, it is crucial that information released for general consumption be properly screened and cleared prior to release. It is equally important that such information be released through a single source, such as the public affairs office. Restricting release of incident-related information through the public affairs office or other designated point will help ensure that frequent, straightforward communication with stakeholders can take place while at the same time controlling rumors and misinformation.

Information released to the public should be handled through a single source representing the organization under experiencing the incident.

Forensic Awareness

Depending on the specific incident, the organization may desire not only to control the incident but also to trace and prosecute the perpetrators in the case of known or suspected criminal activity. It is therefore highly advisable that members of the IRT receive thorough training in procedures for collecting and preserving evidence. Mishandling of evidence can result in an inability to take successful legal action against an attacker or to recover damages following an incident. Computer forensics and evidence handling should be high on the IRT's list of training topics.

POST RESPONSE PROFILE

The IRT's efforts do not end once the incident is resolved. After a rest and recover period, but while the details and the experience are still fresh in the team members' minds, they should examine the incident from start to finish, both formally and informally to evaluate every aspect of the response.

At the conclusion of each incident, the team should be assembled and a formal debriefing and review of the incident should be carried out. This debriefing should include a complete review of the team and its handling of the incident, including its adherence to policy and its technical performance. Each team member should participate individually and as a member of the group. Their recollections, thoughts, ideas, and reactions as to how the incident was handled and how the team performed should be documented and preserved. The IRT members themselves are the best source of data about the weaknesses and strengths of the team, and that data must be captured if the team is to improve and grow in skills and confidence.

Data collected during this review process should form the basis for improving the team. This information provides input to what should be a continuous cycle involving planning, preparation, training, responding, and evaluating. Shortfalls in training, skills, equipment, access, policies, and authority will become evident through this process. These lessons learned are the best mechanism for maintaining a good IRT and improving it over time.