GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Using the FEMA Incident Command System to manage Computer Security Incidents

A paper submitted for GIAC Security Essentials Certification July, 2004.

By Charles Morris

Written under GIAC GSEC Practical Assignment version 1.4b, Option 1

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Abstract

The Information Security industry has made great strides in the past few years. There are now Best Practices and standards to which the industry can refer and formal training has taken the place of the self training, which frequently came by way of unpleasant experience. With all of the progress the industry has made creating Standards of Ethics, Best Practices list, and Gold Standards, one key area of Information Security that seems to have been missed is how to set up and run a Crisis Management team. In this paper we will explore the Crisis Management system that I propose will be the ideal solution for the Information Security industry, the FEMA Incident Command System.

We will begin our discussion with a brief overview of what the Incident Command System is, where it came from and how it is used in the Public Safety area. After establishing an understanding of the basics of the Incident Command System we will apply it to the Information Security field by implementing a Computer Incident Response Team and a Disaster Recovery Team in an Incident Command System frame work. It is believed that as we explore this very powerful management system the benefits will quickly become obvious; however, we will spell out a few benefits and address a few common objections to the use of the Incident Command System in the conclusion.

What is the Incident Command System

The FEMA Emergency Management Institute defines the Incident Command System (ICS) as a "model tool for command, control and coordination of a response and provides a means to coordinate the efforts of individual agencies as they work toward the goal of stabilizing the incident..."[1] The ICS is also highly scalable, it can be used for small routine events or it can grow into a large organization capable of managing extremely large disasters.[2]

The ICS was originally developed during the 1970s in Southern California to address multi agency response to wild fires. Since then use of the ICS has spread far beyond the fire fighting community; versions of the ICS have been developed for Medical Emergencies, Search and Rescue (SAR) and Hazardous Materials (HAZMAT) Incidents. As of January 2004,"... ICS is used by an overwhelming number of agencies."[3] In fact, federal law requires that all

---

[1] FEMA. Emergency Management Institute. "Incident Command System" 1998, p1-2. URL: http://training.fema.gov/emiweb/downloads.is195com.pdf

[2] FEMA, p 2-2.

[3] Gregory Banner, "The Incident Command System. How Civilians 'Think Purple'", Army Magazine, January 2004. URL: http://www.ausa.org/www/armymag.nsf/0/434F9Da045FDD55D85256DFF00516535?OpenDocument

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

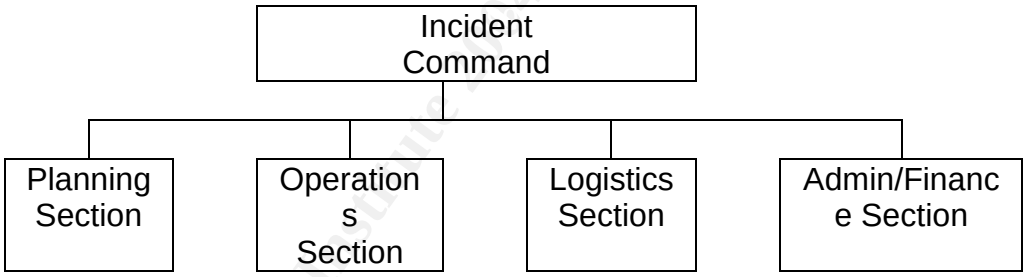
HAZMAT incidents be managed using the ICS.[4] The United States Coast Guard formally adopted the ICS for all of its response operations in August of 1998.[5]

The ICS was developed to meet the following requirements;[6]

1. The system must be organizationally flexible to meet the needs of incidents of any kind and size.
2. Agencies must be able to use the system on a day-to-day basis for routine situations as well as for major emergencies.
3. The system must be sufficiently standard to allow personnel from a variety of agencies and diverse geographic locations to rapidly meld into a common management structure.
4. The system must be cost effective.

How does the ICS Work?

The Incident Command System is built around nine basic principles; common terminology, a modular organization, integrated communications, unity of command, a unified command structure, consolidated Incident Action Plans (IAP), a manageable span of control, designated incident facilities and comprehensive resource management.[7] By applying these principles we arrive at the five basic functions or components of the ICS; Command, Planning, Operations, Logistics and Finance/Administration.[8] These functions provide the basic modules from which any ICS response organization is built.



From FEMA ISC-195 Incident Command System

Incident Command

---

[4] FEMA, p.1-2
[5] USCG. "Incident Command System", (No publication date) URL: www.uscg.mil/hq/g-m/mor/articles/ics.htm
[6] Table from National Interagency Fire Center. "The Incident Command System (ICS)", (no publication Date). URL: www.nicfc.gov/fireinfo/ics_desc.html
[7] FEMA p. 1-16
[8] FEMS p. 1-8

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Incident Command develops and implements an Incident Action Plan[9], and exercises overall responsibility for the response. The ICS Command may take two forms; a single command, in which a single individual acts as Incident Commander, or a Unified Command, under which leaders from the various responding agencies share command. Regardless of the command structure, a command staff may be set up to assist the command.

Incident Action Plan (IAP)
One of the basic roles of Command is to establish an Incident Action Plan (IAP). The IAP defines the objectives and support activities of the response.[10] When responding to smaller short term incidents, the IC may not take the time to establish a written IAP. Larger more complicated Incidents, those that involve multiple agencies, or require a shift change should have a written IAP.[11]

A consolidated Incident Action Plan is an IAP used under a Unified Command structure to coordinate the response actives of multiple independent agencies.

Incident Commander
The Incident Commander is the focus of the command function, "Incidents, no matter their size, are commanded by a single individual, the Incident Commander."[12] When responding to small events, all ICS functions may be retained by the IC. Under this single command system the IC exercises direct control of all aspects of the response. It should be noted that each of the four subordinate functions still exist, they are simply carried out by the IC.[13]

Unified Command
When an Incident's scope crosses jurisdictional or geographic limits a Unified Command (UC) system is often used to bring "... together the 'Incident Commanders' of all major organizations involved to coordinate an effective response while at the same time carry out their own jurisdictional responsibilities."[14] Under Unified Command individual agencies do not give up their jurisdiction; instead each Incident Commander has control of his agency's response, which is coordinated with those of the other agencies. In practice the

---

[9] FEMS p. 1-9
[10] FEMA p. 1-13
[11] FEMA p. 1-13
[12] Walter Green. "The Incident Command System for Public Health Disaster Responders", a paper presented at the August 2002 meeting of the Public Health Task Group, Richmond Metropolitan Medical Response System, Richmond Va., August 2002, URL: http://www.richmond.edu/~wgreen/conf4.pdf
[13] Dispatch Monthly Magazine. "What is the Incident Command System (ICS)?," (no publications date) URL: www.911dispatch.com/ics_describe.html
[14] USCG. "2001 Incident Management Handbook", United States Coast Guard, 2001. URL: www.uscg.mil/hq/g-m/mor/media/chapter6.pdf

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

UC system works fairly well, conflicts are minimal, and are usually solved quickly by the various IC's working together. On the occasion that a serious conflict arises the Incident Commander from the lead agency has the final say.[15]

For UC to work all agencies must work according to the Consolidated Incident Action Plan set by the Incident Command. To facilitate implementation of the IAP all response action is handled under a single Operations Section Chief.[16]

Command Staff
The Command Staff exists to assist Command. Depending on the situation, the IC, at his discretion, may appoint an Information Officer, a Safety Officer, or a Liaison Officer.[17]

Safety Officer
The Safety Officer assists the IC by assuring the safety of responders and the public during the response. The Safety Officer may himself have assistants who represent multiple agencies. The Safety Officer may take action to "...mitigate or eliminate unsafe condition, operation or hazard."[18]

Information Officer
The Information Officer assists the IC by dealing with all information releases about the Incident.[19] There will only be one Information Officer per Incident, including Incidents that fall under a Unified Command structure. The Information Officer may have assistants who represent multiple agencies.[20]

Liaison Officer
The Liaison Officer assists the IC by providing a contact with organizations that do not become part of the ICS structure.[21]

Unity of Command and Span of Control

One of the most important aspects of Command is how it is applied. Under the ICS, two principles define how Command and Control is exercised; these are Unity of Command and Span of Control.

---

[15] USCG. "2001 Incident Management Handbook"
[16] FEMA p. 1-13
[17] FEMS p. 1-13
[18] U.S. Department of Labor. Occupational Safety & Health Administration. "Incident Command System (ICS), Safety Officer", (no publication date) URL: www.osha.gov/SLTC/etools/ics/safe_off.html
[19] FEMS p. 1-10
[20] U.S. Department of Labor. Occupational Safety & Health Administration. "Incident Command System (ICS), Information Officer", (no publication date) URL: www.osha.gov/SLTC/etools/ics/info_off.html
[21] Green, p5.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Unity of Command
Unity of Command (UOC) dictates that each person within the ICS structure report to only one person.[22]

UOC makes clear that during the Incident Response, individuals report to their ICS supervisor only; normal reporting chains are suspended for the duration of the response. This formalization of the chain of command is often vital when responders from multiple organizations are involved.

Span of Control
Span of Control refers to the number of responders who can be effectively supervised by a single individual. The ICS, as used in emergency response situations, defines the Span of Control as between three and seven, with five direct reports being the optimum.[23] In practice, the Span of Control should be set to the number that a supervisor can effectively account for.[24]

Functional Sections

Depending on the scope of the Incident, the IC may choose to manage all of the functions himself or he may choose to create a Section to manage one or more of the ICS basic components. [25] Each section is headed by a Chief, to whom authority to manage that part of the Incident is delegated, including the authority to grow or shrink his section as needed.[26] The Section Chiefs together make up the General Staff and report directly to the Incident Commander.[27] A more detailed explanation of the ICS subordinate components is provided below.

Planning Section

The Planning Section may be set up when a response will be complicated or will require a long term response. The Planning Section is the eyes and ears of the Command; it is responsible for the collection and dissemination of information about the Incident within the response organization. The Planning Section may also be tasked with the creation of a proposed Incident Action Plan (IAP)[28], which will be reviewed and approved by Command.

The planning section may have four subordinate units, as needed. These are the Resource Unit, which tracks all personnel, the Situation Unit which provides

[22] FEMA p. 1-13
[23] FEMA p. 1-13
[24] Green, p8.
[25] Dispatch Monthly Magazine. “What is the Incident Command System (ICS)?”
[26] FEMA p. 1-16
[27] FEMA p. 1-10
[28] FEMA p. 1-10

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

all "intelligence information" for the Incident, the Documentation Unit, which maintains the official documentation for the Incident and the Demobilization Unit, which sets up the demobilization plan.[29]

Operations Section

The Operations Section actually implements the Incident response. All response operations are handled through the Operations Section, which is responsible for the implementation of the Incident Action Plan (IAP).[30]

The Operations Section, as the arm of the ICS organization actually carrying out the Incident response, may set up subordinate branches, divisions or group organizations as needed.[31]

Division
A Division is the subordinate organizational unit that has responsibility for a geographic region.[32]

Branch
A Branch is the subordinate organizational unit that has responsibility for a major part of the Incident response, which may be either a functional or geographic area.[33]

Group
A Group is the subordinate organizational unit that has responsibility for a specific functional area of the response.[34]

Logistics Section

The Logistics Section provides or coordinates all of the facilities, services, and materials needed for the response. Logistics become more important as an Incident grows. A response of any significant length or requiring much in the way of material support will need a Logistics Section. It should be noted that the Logistics Section exists to support the responders as they carry out their duties. For example, the Food and Medical Units, under the Logistics Sections provide services to responders, not to victims of an Incident.[35]

[29] National Interagency Fire Center. "The Incident Command System (ICS)"
[30] FEMS p. 1-11
[31] National Interagency Fire Center. "The Incident Command System (ICS)"
[32] FEMS p. 2-5
[33] FEMA p. 2-5
[34] FEMA p. 2-5
[35] FEMA p. 1-11

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The Logistics Section may have up to six subordinate units; the Supply Unit, which handles all ICS supplies, the Facilities Unit, which sets up and maintains the facilities used during the Incident, the Ground Support Unit, which provides and maintains all ground transportation, the Communications Unit, which provides all communications, a Food Unit, which provides food and water to the responders during the Incident, and a Medical Unit to provide medical assistance and treatment to responders during the Incident.[36]

Finance/Administration Section

The Finance/Administration Section tracks all costs associated with the Incident response.[37] This function is often overlooked in the response to an Incident, but is vital if any attempt to recover the expense cost is to be made.

The Finance/Administration Section may include a Time Unit, to track personnel time, a Procurement Unit, to handle purchase and leases needed for the response, a Compensation/Claims Unit, to handle injury and property claims and a Cost Unit, which tracks the Incident cost.[38]

The Logistics and Finance/Administration Sections function together to address two of the key principles of the ICS, Designated Incident Facilities and Comprehensive Resource Management.

So far we have discussed the implementation of seven or the nine basic principles of the ICS. Two principles remain, Common Terminology and Integrated Communications. These principles, while they do not fit into our description of the implementation of an ICS organization, are in fact critical. After all, how can you set up and run anything if you cannot get clear, understandable messages to your colleagues?

Common Terminology and Integrated Communications

Because they are critical, both Terminology and Communications should be addressed during the Planning stages of ICS implementation. All potential responding agencies should agree well ahead of time, on the types of communications channels they will use and on the language of the response.

Common Terminology

A Common Terminology is the language of the Incident response and is essential in any response.[39] By establishing a common working vocabulary

[36] National Interagency Fire Center. "The Incident Command System (ICS)"
[37] FEMA p. 1-11
[38] National Interagency Fire Center. "The Incident Command System (ICS)"
[39] FEMA p. 1-12

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

before the need arises, the different responding organizations will be able to communicate useful information with a minimum of confusion. A good example is the elimination of "ten-codes", which often vary from agency to agency.[40]

Integrated Communications
Integrated Communications refers to a system under which all response communications are carried out under a single communications plan. A typical Communications Plan will specify standard operating procedures, technology, frequencies and terminology. The ICS also specifies that all response communications should be in clear text.[41]

How can the ICS be used in Computer Security?

Like the fire fighters who created the ICS Information Security, professionals frequently find themselves planning for or actually dealing with, incidents that reach beyond the scope of the their normal duties. Frequently, these Incidents require the coming together of experts from various parts of the organization; the ICS provides a predefined method for putting these additional assets to work, with a minimum of confusion. Computer Incident Response Teams (CIRT's) and Disaster Recovery Teams are just two Information Technology undertakings that could benefit from the use of the ICS.

Using the ICS to organize a CIRT

The members of the Computer Incident Response Team (CIRT) are the people an organization turns to when a security event rises to the level of an Incident. Michelle Borodkin's, in her paper, "Computer Incident Response Team", defines a CIRT as "A carefully selected and well-trained group of people whose purpose is to promptly and correctly handle an Incident so that it can be quickly contained, investigated and recovered from."[42] Borodkin suggest that representatives of the following departments be included as members of the CIRT; [43]

Management
Information Security
IT/MIS
IT Auditor
Security
Attorney

---

[40] T. W. Conner. "Incident Command System for Law Officers", Federal Bureau of Investigations, 1997. URL: www.fbi.gov/publications/leb/1997/sept497.htm
[41] FEMA p. 1-12
[42] Michelle Borodkin. "Computer Incident Response Team", SANS Institute, 2001. URL: http://www.sans.org/rr/papers/index.php?id=641
[43] Borodkin

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Human Resources
Public Relations
Financial Auditor

Pulling all of these professions together and getting them all working toward the same goal is no small task. Each of the departments represented has its own structure, hierarchy and priorities, what is needed is some unifying system to bring each of these into harmony for the good of the organization as a whole. The ICS, because of its modular nature, can make bringing everyone together much easier.

Using the ICS, and working from Borodkin's list of CIRT members we might organize our CIRT for a major security event as follows;

Command Section
The CIRT would probably have a Unified Command, with a senior member of management, a senior IT representative and a representative from the production departments most directly impacted. If the Incident had any impact on equipment that could affect safety (production robots, medical equipment, Power Plant, etc.), a Safety Officer would be appointed, probably from Human Resources or the Safety Department. Financial institutions or firms that must report such issues to the public will need to appoint an Information Officer, probably from Public Relations. If outside assistance is required from a vendor or local utilities (or police), a Liaison Officer might be appointed. This will probably be the company employee who has the most experience with that vendor.

The Unified Command section for the CIRT will look like this:

Unified Command:	IT/MIS	
	Management	
	Operating Department 1	
	Operating Department 2…	
Command Staff:	Safety Officer	Human Resources or Security
	Information Officer	Public relations
	Liaison Officer	Vendor contact person.

Planning Section
The Planning section will probably include members from the most departments. Remember from our earlier discussion, it is the Planning Section that gathers information about the event and formulates the plan for the response; everyone who will be affected should be represented. The Planning Section will include at a minimum, representatives of Management, IT, the production department(s)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

most directly impacted, and if available, an IT Auditor should be part of the Planning Section, as should a knowledgeable person from Human Resources.

Planning Section assignments;

Resource Unit	Human Resources
Situation Unit	IT Auditor IT/MIS Management Security IS Security Attorney
Documentation Unit	IS Auditor Attorney Financial Auditor

Demobilization Unit - probably would not be used for most CIRT situations.

Operations Section
As the arm of the ICS structure that will actually be doing the work of the response, the Operations section will probably have representatives of every department involved. There may be a Network Division, a Server or Router Branch, and possible subordinate units from the Operating Departments all working together to address the response. The key here will be that they will all be working together, according to an Integrated Action Plan, as approved by the Command Section.

Logistics Section
Logistics provide everything needed for the response except the people. The Operations Section draws its resources from the Logistics Section as needed. In most CIRT situations the Logistics Section would consist of a Supply Unit and possibly a Communications and Food Unit. A Facilities Unit might be needed if the Incident continued over an inordinately long time frame.

A CIRT Logistics Section will include a member of the MIS/IT, Human Resources, and Purchasing departments. If additional Facilities are needed, the Command Sections may need to make arrangements with Management to establish a Facilities Unit.

Logistics Section Assignments:

Supply Unit	Management

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Communications Unit	MIS/IT
Food Unit	Human Resources
Facilities Unit	Management Security

Finance Administration Section
The Finance Administration Section will track the cost of the Incident and will make any purchases necessary to the response, including the purchase of contract services. The employment of a Finance Administration section will help to document the cost of the Incident, and will help to maintain reasonable control over expenditures during the event.

Many CIRT responses will not require the use of a Compensation/Claims Unit; the probability of bodily injury is usually low. However, any organization which might have to deal with litigation as a result of a Computer Incident, Hospitals, Utility Companies, Internet Service Providers, etc. would be well advised to implement one.

Finance Administration Section Assignments:

Time Unit	Human Resources
Procurement Unit	Management Purchasing
Compensation Claims Unit	Financial Auditors Attorney
Cost Unit	Financial Auditors

Disaster Recovery Plans

The Disaster Recovery Plan (DRP) is another aspect of Information Technology that can benefit from the use of the ICS. When looked at from the over view of the organization as a whole, it is clear that the IT Disaster Plan is simply one part of a much larger plan designed to restore the firm's ability to do business. It has been argued that a full Business Continuity Plan consists of a Business Resumption Plan, Occupant Emergency Plan, Incident Management Plan, Continuity of Operations Plan, and a Disaster Recovery Plan.[44] Obviously, a

[44] Chad Bahan. "The Disaster Recovery Plan", SANS Institute, 2003 URL: http://www.sans.org/rr/papers/index.php?id=1164

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

modular management system like the ICS would be of great value when trying to carry out such a complicated endeavor.

In this section we will explore how the ICS can be used to organize a Disaster Recovery Plan working from an existing published DRP organizational structure, the one used by the University of Arkansas, published on the Internet at www.uark.edu/staff/drp/drpdr006.htm. Using this very good DRP structure, we will examine how the ICS might be used to modify the plan, bringing it into compliance with the overall ICS philosophy, and reducing double work for some responders.

The University of Arkansas defines eight Disaster Recovery Teams; [45]

Recovery Management Team
Damage Assessment Team
Facility Recovery Team
Network Recovery Team
Platform Recovery Team
Applications Recovery Team
Computer Operations Team
Administrative Support Team

In addition, seven key positions are spelled out.[46]

Recovery Manager
Facilities Coordinator
Technical Coordinator
Administrative Coordinator
Network Coordinator
Applications Coordinator
Computer Operations Coordinator

Under the University Plan these individuals make up the Recovery Management Team, with the Recovery Manager being the leader.[47] Under the ICS this would correspond, roughly, to the General Staff and the Incident Commander.

Other assignments are as follows; [48]

---

[45] University of Arkansas. "Disaster Recovery Plan, Disaster Recovery Teams (BRPDROO6)." 2002. URL: www.uark.edu/staff/drp/drpdr006.htm

[46] University of Arkansas. "Disaster Recovery Plan, Disaster Recovery Teams (BRPDROO6)"

[47] University of Arkansas. "Disaster Recovery Plan, Disaster Recovery Teams (BRPDROO6)"

[48] University of Arkansas. "Disaster Recovery Plan, Disaster Recovery Teams (BRPDROO6)"

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Technical Coordinator	Damage Assessment Team Platform Recovery Team
Facility Recovery Coordinator	Facilities Recovery Team
Network Recovery Coordinator	Network Recovery Team
Applications Coordinator	Application Recovery Team
Computer Operations Coordinator	Computer Operations Team
Administrative Coordinator	Administrative Support Team

This is actually a very good system, even when judged using the ICS model. There are, however, a few weaknesses that an ICS based system would eliminate:

1. There is no provision for a formal Integrated Action Plan.
2. The assignment of the Technical coordinator to both the Damage assessment and platform Recovery teams violates Unity Command.
3. There are too many people on the General Staff
4. No provision has been made for providing service to the responders; they are required to provide for their own needs at the same time they respond to the disaster.

Using the ICS the DRP organization at the University Of Arkansas can be revised to eliminate these issues. An ICS version of the Plan is presented below.

Command	Recovery Manager	
Command Staff	Safety Officer	Public Safety
	Information Officer	Public relations
	Liaison Officer	Vendor contact person

Planning Section;

The Planning Section would be an addition to the University Plan. The Plan would require modification to nominate a Planning Section Chief, and to accommodate the new section.

Resource Unit	Human Resources
Situation Unit	Damage Assessment Team
Documentation Unit	IS Auditor Attorney Financial Auditor

Demobilization Unit – for a campus-wide emergency a demobilization unit would

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

be of great benefit, and would include all members of the Planning Section.

Operations Section
The position of Chief of Operations would probably be assigned to the individual who had been listed as Technical Coordinator with the Network, Platform, Applications and Computer Operations coordinators reporting to him.

Operations Section	*Division*	*Branch*
	Computer Operations Team	Network Recovery Team Platform Recovery Team Applications Recovery Team
	Facilities Recovery Team	

Logistics Section
The Logistics Section would be an addition to the University Plan, and would require the plan to nominate a Logistics Section Chief. The members of this section would function to support the rest of the responders as they deal with the disaster. Depending on the nature of the disaster any of the teams in the Operations section might be moved to Logistics.

Logistics Section Assignments:

Supply Unit	Management
Communications Unit	MIS/IT
Food Unit	Human Resources
Facilities Unit	Management Public Safety

Finance Administration Section

The University Planned Administrative Support team would fall into the Finance Administration Section, which would be headed by the individual designated the Administrative Coordinator in the University Plan.

Finance Administration Section Assignments:

Time Unit	Human Resources
Procurement Unit	Management

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

	Purchasing
Compensation Claims Unit	Financial Auditors Attorney
Cost Unit	Financial Auditors

We have now reorganized the University of Arkansas DRP according to the ICS, in doing so we have addressed each of the weaknesses pointed out earlier;

1. We have created a Planning Section charged with the evaluation of the situation and the formulation of an Integrated Action Plan.
2. We have eliminated possible confusion by removing a violation of Unity of Command. Under the revised organization no one is 'wearing two hats'.
3. We have added two positions to the General Staff but have reduced the size of the staff, ensuring a manageable Span of Control.
4. By adding a Logistics Section we have created a management infrastructure to support the responders as they go about the business of dealing with the disaster.

Not Just Moving Boxes Around

Many readers may see the discussion of the management model as simply an exercise in “moving boxes around on a piece of paper.” Nothing could be further from the truth. The author has been present in the data center of a multinational, multi-billion dollar corporation when the IT staff could not make a basic decision to begin a repair. While they debated, the company lost approximately two million dollars an hour. The issue was finally settled when a non-IT manager assumed control and demanded that something be done, after wasting 2 days. Compare that to the Disaster Relief programs that the author has also been involved in, some of them covering as many as five states and involving hundreds of people, aircraft, and ground assets. Most of the people, well over sixty percent, were volunteers and much of the equipment was privately owned. The volunteers did a much better job of getting the job done than all of those technical experts because they had a plan and clear leadership. Management is important, it can make or break any endeavor, and it should be taken seriously by everyone involved.

Conclusion

Benefits and Barriers

The Information Security profession needs a standard Crisis Management model to provide a framework for the various technical and procedural standards the

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

industry is developing. The ICS, as a nationally standardized model, with decades of ongoing development is ideally suited to fill that role. A few of the benefits the ICS can provide are listed below;

1. The ICS provides a well proven, public domain crisis management system that can scale up and down as needed.
2. The ICS structure helps crisis managers to cover the less obvious parts of the response. The Logistics and Finance Administration Sections in particular will be very helpful.
3. The ICS provides a structured way of pulling highly skilled individuals together leveraging their existing talents for the good of the operation as a whole.
4. The existence of a formal management structure, even for the types of crisis that cannot be predicted, will assist in securing management support for the CIRT, Disaster Planning process.

There will of course, be objections to the implementation of the ICS. Fortunately many of these have already been encountered as the ICS moved from the Fire Management to hospital and other types of crisis management uses. We will discuss a few of the more common objections with recommended answers below. It should be noted that these are objections that the author has encountered and the solutions that he has used. Others may have had similar experiences.

Possible barriers to implementation and solutions

1. "I'm not in the Army, I don't do Command!" This objection actually comes up fairly routinely. If an objection over the name pops up simply change it to the Incident Coordination System, etc. If it is necessary to change the name of the system try to keep the acronyms and initials the same, this will help when looking for public domain training materials and when working with other agencies that use the ICS.

2. "Not invented here." Many technical experts are wary of systems and methods that were developed outside of their specific field, and the computer business is no exception. ICS advocates must demonstrate that the process of crisis management is as much a technical skill with best practices, protocols, and systems just as detailed as those of the IT industry. When these things are understood, the IT personnel will reach a level of professional respect that will compel them to accept and build on the decades of hard work put in by our colleagues in the Public Safety field.

3. "This will let non-technical people be in charge!" In some cases that is true. Under the ICS, each member would fall into the system where they can do the most good. In some cases that means that a talented manager might be designated IC, while the outstanding technical member served as Planning or

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Operations Chief. This objection is usually dropped when everyone is reminded that the ICS is a temporary structure, designed to meet a specific goal, for the good of everyone involved.

Final Word

The ICS is a well tested crisis management system that is ideally suited to serve the needs of the Information Security industry. The author recommends that ICS training be included as a standard part of all Information Security training. ICS training will be especially valuable for those charged with developing or implementing a CIRT or a Disaster Recovery Team.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Bibliography

Bahan, Chad. "The Disaster Recovery Plan." SANS Institute, 2003
http://www.sans.org/rr/papers/index.php?id=1164

Banner, Gregory. "The Incident Command System: How Civilians "Think Purple"". ARMY Magazine, January 2004
http://www.ausa.org/www/armymag.nsf/0/434F9DA045FDD55D85256DFF00516535?OpenDocument

Borodkin, Michelle. "Computer Incident Response Team." SANS Institute, 2001
http://www.sans.org/rr/papers/index.php?id=641

Conner, T.W. "Incident Command System for Law Enforcement", Federal Bureau of Investigations, 1997.
http://www.fbi.gov/publications/leb/1997/sept497.htm

Dispatch Monthly Magazine. "What is the Incident Command System ICS)?" Dispatch Monthly Magazine, No publication date
http://www.911dispatch.com/ics/ics_describe.hml

Federal Emergency Management Agency. Emergency Management Institute. 1998. Incident Command System. IS195.
http://training.fema.gov/emiweb/downloads/is195comp.pdf

Green, Walter. "The Incident Command System for Public Health Disaster Responders" a paper presented at the August 2002 meeting of the Public Health Task Group, Richmond Metropolitan Medical Response System, Richmond Va., August 2002,
http://www.richmond.edu/~wgreen/conf4.pdf

National Interagency Fire Center, "The Incident Command System (ICS)", National Interagency Fire Center, No publication date
http://www.nifc.gov/fireinfo/ics_disc.html

United States Coast Guard, "Incident Command System", United States Coast Guard, No publication date
http://www.uscg.mil/hq/g-m/mor/articles/ics.htm

United States Coast Guard. "2001 Incident Management Handbook", United States Coast Guard, 2001.
http://www.uscg.mil/hq/g-m/mor/media/chapter6.pdf

United States Department of Labor. Occupational Safety & Health Administration, "Incident Command System (ICS), Safety Officer", United States Department of Labor, No publication date

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

http://www.osha.gov/SLTC/etools/ics/safe_off.html

United States Department of Labor. Occupational Safety & Health Administration, “Incident Command System (ICS), Information Officer”, United States Department of Labor, No publication date
http://www.osha.gov/SLTC/etools/ics/info_off.html

University of Arkansas. “Disaster Recovery Plan, Disaster Recovery Teams (DRPDR006), University of Arkansas, 2002.
http://www.uark.edu/staff/drp/drppdr006.htm

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.