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
"Hacker Tools, Techniques, Exploits, and Incident Handling (Security 504)"
at http://www.giac.org/registration/gcih

Using the Incident Command System for Computer Incident Handling

Jonathan Clemens

July 18, 2000

The Incident Command System (ICS) was designed for use during large-scale incidents such as fire, flood, and other natural or manmade disasters. It was designed to manage standardized and interchangeable resources such as firefighters and bulldozers, but also be flexible enough to deal with the differing needs and requirements of specialized equipment such as aircraft. During computer incidents, economic livelihoods may be "on the line," but lives and physical property generally are not at risk.

Fundamentally, however, computer incidents are just that—incidents. Virus infections, computer break-ins, and other computer threats share many traits in common with the other sorts of incidents which ICS has traditionally been used to manage. Those of us who are fundamentally white-collar computer system administrators, security specialists, and incident response specialists would do well to learn from the lessons of the blue-collar professionals who've traditionally handled our nation's crises. Their efforts to improve reaction and coordination can yield dividends to those of us striving to match their level of response and professionalism as we deal with new types of incidents.

Since this document is targeted towards computer professionals who need to respond to incidents, rather than to emergency services personnel who are well versed in ICS, a familiarity with computer incident handling is assumed, while a familiarity with ICS is not.

The first step in understanding how ICS can apply to computer incidents is to gain a basic understanding of ICS. Use one of the following sources for an ICS Orientation. The link at from the U.S. Coast Guard Institute is roughly equivalent to Unit 1 from the FEMA Emergency Management Institute course IS-195.[1]

U.S. Coast Guard Institute

Federal Emergency Management Agency

ICS Organization

Command

The command organization is responsible for setting objectives and priorities. Four positions (with appropriate deputies and assistants, if needed) comprise this part of the organization.

Incident Commander

[1] I really am serious about you reading these. If you breeze past these URLs and my document doesn't make much sense, don't blame me.

© SANS Institute 2000 - 2005 Author retains full rights.

When more than one individual works together to handle a computer incident, someone must be in charge. The most key position to staff properly in an ICS response is the Incident Commander.

The choice of an Incident Commander to handle a computer incident response is often difficult and the available personnel are less than optimal. When planning[2] who will fill the role of Incident Commander during a future incident, management should look for potential Incident Commanders who are:

- willing to be in charge,
- familiar with the information technology assets at risk,
- familiar with the business value of the systems at risk,
- able to make good decisions quickly, and
- trusted by management to fulfill this critical role.

First, an Incident Commander must be willing to step into the maelstrom in an attempt to mitigate its impact. This is a very different thing from working before the fact to prevent an incident from happening. The difference between a computer security administrator and a computer incident handler is somewhat akin to the difference between a building inspector and a firefighter. A building inspector, like a security administrator, needs to be thorough and persistent in order to minimize risk. A computer incident handler or firefighter needs to be well trained to respond with tools and procedures appropriate to the situation to minimize further damage after an incident is already underway. If a competent but unsuited computer professional is thrust into a crisis management role, it may result in undue stress upon the individual, in addition to less than optimal incident management.

Second, emergency response organizations are managed by men and women who have come up through the ranks and have previously participated in many incidents of various kinds. The same cannot be said of most information technology organizations. Fire or police lieutenants are fire fighters or police officers first, respectively, and only selected for their increased responsibility after demonstrated competence and aptitude for further leadership.

Information Technology managers, on the other hand, often come from general management and may never have had the technical skills that their subordinates will be called upon to use. Alternatively, such a manager may have demonstrated technical competence earlier in his or her career in a facet of information technology that differs markedly from the technical skills which his or her subordinates will be engaging in incident handling. In neither case would such a manager be an optimal choice for Incident Commander. The Incident Commander must be able to knowledgeably evaluate the recommendations of his or her staff, especially when members of the incident response team look to him or her to resolve a dispute during the stress of an ongoing incident.

[2] Yes, *planning*. ICS requires adequate planning and preparation before it can yield any benefits to a responding organization. If you intend to use ICS to manage computer incidents, then this document alone cannot adequately prepare you for

© SANS Institute 2000 - 2005 Author retains full rights.

Third, an Incident Commander must have a clear view of the organization's priorities and how the actions taken in response to an incident will support those priorities. If an Incident Commander chooses to pursue a course of action at odds with organizational priorities, disaster can result. For example, if a company values its image of absolute financial integrity, it would be inappropriate for an Incident Commander to allow an attacker to download customer credit card information in hopes of later prosecuting the perpetrator. While that example may seem clear cut, real life examples may be much subtler.

Fourth, an Incident Commander must be able to exercise good judgement rapidly. Many IT professionals are temperamentally unsuited for this. Some may be too action-oriented, failing to plan adequately; others may be too analysis-oriented, failing to act appropriately to mitigate further damage. Individuals with such traits who enter the emergency services fields tend to adapt or pursue other career choices before being promoted into positions of responsibility.

Fifth, an Incident Commander must have management's confidence that he or she will manage an incident competently. This is absolutely critical if the Incident Commander is to be allowed the freedom to make decisions that may affect an entire enterprise without consulting higher management. While management has responsibility for the continued operation of an organization's information assets, the proper function of an incident command system demands that appropriate authority be delegated to a trained individual, who will most likely not be a senior corporate officer, and may not even directly manage other employees.

While these traits are listed as specifically being appropriate for an Incident Commander, they are, to some extent, desirable for section chiefs, command staff, and other key incident response personnel.

Information Officer

An incident, by its very definition, has the potential to affect a large number of people. A serious traffic accident on a crowded freeway may only kill or injure a few individuals, but dozens of responders will be involved and thousands of motorists will probably be inconvenienced.

Computer incidents have the potential to both have numerous victims, as well as numerous affected persons. Any of the 1999-2000 Outlook mail worms can demonstrate this fact: many people double clicked a malicious attachment, and many more were affected by the unwanted mail, unresponsive servers, and downed Internet mail links.

While an information officer may be completely unnecessary—or even inappropriate—for a penetration incident, an information officer should be used at any incident that has the potential to affect individuals other than the direct victims and incident responders.

In the case of a denial of service incident, the information officer may need to use out-of-band communications to let the affected individuals know how the incident affects them. During various Outlook mail worm incidents, Intel used Intranet articles and fliers passed out at building entrances to update the employee community on the status of the incident and the steps they

© SANS Institute 2000 - 2005 Author retains full rights.

needed to take if they encountered an infected attachment. This not only kept the individuals informed, but by proactively communicating the status to the whole organization, the effect upon the IT technical assistance call center was lessened.

If a computer incident becomes newsworthy, (and that decision rests with the news media and not the incident management staff) the Information Officer must engage the news media and provide them with as much timely, accurate information as is appropriate. The Information Officer should provide enough information to forestall speculation that could be more damaging than the truth, but not internal conjecture or other information that would exacerbate the media attention, reputation damage, and/or legal liability stemming from the incident.

An Information Officer does not need to be permanently attached to the incident handling team. Many sizeable organizations have public affairs or internal communications organizations. If your organization has such a team, this mission will be much better suited to their training. If not, a senior manager who has experience in public speaking and understands these goals can be a good alternative.

Safety Officer

Computer incidents will rarely involve direct threats to people's lives—and it's hard to imagine a computer incident which poses a serious threat to the health and safety of responders. The possibility for office accidents always exists, and may be exacerbated by the adrenaline rush of an ongoing incident. For example, an enthusiastic responder might try to lift too much weight or run too fast in a hurry to complete a simple task. While the possibility of this sort of reaction or accident shouldn't be minimized, there is probably not a need to assign an individual to review the planned actions for possible pitfalls of this nature.

Instead, the safety officer's role in a computer incident may be more focused on damage to the affected system that might be caused by the incident response team's actions. A good IT organization will already have some sort of a change management process in place,[3] and that change management process will almost certainly not be responsive enough to handle changes requested during an incident. Because the system's function will be more at risk from the incident than from failure to use change management, change management guidelines will almost certainly need to be suspended.

This is the lesser of two evils, obviously, and therefore an individual should be assigned to review the system changes requested by the incident response staff, and advise the Incident Commander of the risks involved. In essence, the Safety Officer becomes a one-person change management system for the duration of the incident. The Safety Officer would retain the ability to stop any unsafe act, but the focus of his or her work would be on the "safety" of the information systems affected by the incident, rather than on the safety of the responders.

Liaison Officer

[3] In fact, it's rather hard to imagine an information technology department implementing an incident response team without benefit of a change management process, but the possibility does exist.

© SANS Institute 2000 - 2005 Author retains full rights.

As with any ICS-managed incident, a Liaison Officer is only necessary if multiple agencies are involved in the response. While it might be unlikely that other agencies' resources will be directly assigned to an Incident Commander, the defensive information warfare community maintains a number of assets, such as CERT and similar organizations, which can be called upon to assist in a computer incident response. If sufficient external contacts warrant the involvement of a Liaison Officer, then he or she should handle those contacts with other assisting agencies.

Operations

The operations section is responsible for executing the Incident Action Plan. The relationship between the Operations and Planning sections merits special attention, since the mix of execution vs. planning involved in computer incident handling will often be reversed from traditional incident handling, where operations take the vast majority of the personnel and effort.

The Relationship between Operations and Planning

The responsibility of the operations section is to direct the tactical actions to meet the incident objectives. The planning section is responsible for the collection, evaluation and display of incident information, maintaining the status of resources, and preparing the Incident Action Plan (IAP) and incident-related documentation.

In incidents traditionally handled by ICS, the operations section is responsible for far more personnel and equipment than the planning section. A dozen men and women may handle all the strategic planning for a major incident which will require hundreds of operational personnel to execute the Incident Action Plan that they generate.

Also, in computer incidents, the type and impact of the incident may never have been seen before, and the proper course of action to mitigate its impact and return the affected system(s) to normal is very often unknown at the start of the incident. Contrast that to a forest fire, where the terrain and weather are variable, but both the planning and operations personnel assigned to the incident will have handled dozens or hundreds of similar incidents. The tools for fighting forest fires may have improved recently, but the fundamental nature of wildfires is fixed by the laws of physics and will not change from one incident to the next.

Because the number of operational personnel required to implement an IAP is so small, and the need for the planning section to deal with many more variables is so likely, the planning section may often eclipse the operations section in size and importance during a computer incident.

Operations in a computer incident

The Operations section's duties are to execute *tactical* solutions. The Incident Commander sets the objectives and priorities, Planning defines what to do in support of those objectives, and Operations executes those actions.

© SANS Institute 2000 - 2005, Author retains full rights.

That doesn't mean, in the scope of a computer incident, that Operations must be relegated to merely typing in commands that Planning dictates to them. While the actual level of specificity in the incident action plan may vary from incident to incident, a competent Operations section should be able to generate, test, and use scripts to deploy solutions provided by the Planning section to all of the systems affected by an incident.

In a small-scale computer incident, the "Operations section" may consist of the one system administrator who is typing on the system console, while a few others look over his or her shoulder. In this sort of an incident, it should be obvious that the system administrator who types best under stress and observation should be selected to actually sit at the terminal.

During a more complex incident, Operations can often take known actions to mitigate the effects of an incident while Planning works on a more permanent solution. For example, if a large web farm is under attack, server administrators can be tending and rebooting the beleaguered systems while network analysts assigned to the Planning section try and isolate the source(s) of the attack.

In such a case, the actions of the Operations section will not stop the attack, but they are essential to mitigate the total effect of the attack: if only the Operations section is responding, the attack can continue until the attacker tires. On the other hand, if only the Planning section is involved, the web farm may be totally out of service until a complete solution is implemented. Neither case is optimal, obviously.

Planning (or Planning/Intelligence)

In light of the above discussion, the roles of the Planning section take on unique and special significance in computer incident handling.

Resources

The resources unit in a traditional incident is responsible for checking in and keeping track of many more personnel than in a typical computer incident. In an incident where the complete ICS structure has perhaps a dozen total individuals, this function can probably be performed as a collateral duty by another person assigned to the planning section—perhaps the planning section chief himself or herself on smaller incidents.

Situation

The situation unit is responsible for keeping the current status of the incident accurately displayed. This position may or may not be appropriate for a computer incident; again, like many other positions, the likelihood that this position will be necessary will increase with the complexity and duration of the incident.

One of the exciting possibilities for computer incident handling is that this position won't necessarily have to move magnets or use grease pencils. Several collaboration technologies exist (e.g., NetMeeting, HTML) which can be used to display the situation to not only those physically

© SANS Institute 2000 - 2005 Author retains full rights.

present in the Incident Command Post, but also to the other responders and authorized people using networked computers. Of course, if the network is unavailable or the incident being handled requires out-of-band communications, then this sort of sharing would not be appropriate or available.

Documentation

The documentation unit is a very, very important function when the computer incident may result in prosecution of a perpetrator. Not only will the cost of the response help trigger damage thresholds for prosecution, but the information collected during the evolution of an incident will be primary evidence. If that evidence is poorly documented or mishandled, any chance of prosecution and conviction will be severely limited.

If the Incident Commander has made prosecution of the person(s) responsible for the incident an incident objective, staffing the Documentation unit should be a high priority. Because the information and evidence collected in the course of a computer incident is so easy to modify and it is so difficult to prove its integrity, simply going back and labeling everything collected after the end of an incident will probably be inadequate for prosecution purposes.

The Documentation unit should receive copies of all evidence collected, when it's collected, and then be responsible for insuring its authenticity and retaining a chain of evidence for all this. While specific techniques for preserving evidence will undoubtedly evolve, adding a footer and then digitally signing online evidence can provide an excellent method for the Documentation unit to prove time of receipt and the integrity of the document after receipt.

Demobilization

Like the resources unit, the Demobilization unit probably does not need to exist as a separate unit during a computer incident. What little demobilization activity needs to happen while the incident response is winding down can generally be handled by other Planning section personnel.

Technical Specialists

Technical specialists are, by default, assigned to the planning section, but can be assigned anywhere. In the context of computer incidents, defining exactly who constitutes a 'technical specialist' can be problematic.

Computer incidents almost always have some facet of newness about them—often times, they are completely new. Unless the rate of change in the information technology industry slows down, it would be unrealistic to expect this to change significantly. A large burden on the planning section is getting a good handle on what, precisely, is happening. This duty could be assigned to the Situation unit, or an alternate unit comprised of technical specialists could be chartered under the planning section to analyze and respond to the incident.

Technical specialists assigned to an incident should vary somewhat based on the nature of the

© SANS Institute 2000 - 2005 Author retains full rights.

incident—malware attack, crime in progress, etc. The best technical specialists assigned to an agency should be collected in order to think through the problem and the appropriate response.

The experts assigned to this team don't need to be experts in ICS—a basic understanding of their place within the hierarchy will suffice. The unit leader,[4] on the other hand, will need to know ICS well enough to make sure that the team's findings and recommendations are constructed into an Incident Action Plan and conveyed appropriately to the Incident Commander and operations section.

Logistics

Since computer incidents are going to be much, much less manpower-intensive than traditional incidents, the need to feed and house responders is going to be significantly less. However, as incidents range into the more complexity and longer duration, a Logistics section—even if only composed of one person—will be essential to keep the incident responders focused on their incident.

Someone has to procure the food and appropriate beverages necessary to keep the incident responders functioning at peak efficiency. Likewise, any non-drill incident will uncover things that should have been procured beforehand, but weren't—Post-It notepads, CD-R media, magnetic tape, whatever it is, someone will have to get it. Rather than trying to plan for every contingency, it's often more appropriate to keep known supplies at hand, and plan on having a responsible Logistics person to comprise the logistics section and trust him or her to procure extraordinary items.

One additional duty that falls to the logistics section and may be especially applicable for computer incidents is the communications team. Cell phones, desk phones, FAX, and email may not require the same degree of interagency cooperation and planning as handheld and vehicle-mounted radios, but communication can still be a problem. Is everyone going to have the IC's cell phone number? That would be a quick way to end up with a dead battery and a frazzled IC! If there is going to be significant cross-location communication, a person should be assigned to the Incident Command Post to facilitate the flow of information throughout the incident response structure.

In a computer incident, one important communication consideration may be to prevent an intruder from detecting that a response is in progress. That can involve out-of-band or encrypted communications. Unless an attacker also controls your PBX, phones can be a reliable, secure, out-of-band communications method. However, when phones are used to communicate information during an incident, incident response personnel must use care to keep and maintain good notes, which will be crucial in both assuring the accuracy of the message and in reconstructing the series of events during an after-action review or subsequent legal proceedings

Finance/Administration

[4] Who may be the Planning section chief in a small incident.

© SANS Institute 2000 - 2005 Author retains full rights.

The finance and administration section initially may not seem all that important in a computer incident. However, current computer crime statutes place dollar thresholds on crimes, and often prosecutors have their own, higher minimum concrete damages that must be demonstrated before charges will be filed as a result of an intentionally-caused incident. This function can often be filled after the fact, based on the records kept by the documentation unit.

Since computer incidents don't often involve damage to equipment or injuries to personnel, the compensations/claims unit is probably not necessary. Likewise, sine most responders will be salaried and responses approaching a pay period in duration are currently very rare, the Time Unit is probably unnecessary. Procurement of "vendor contracts, leases, and financial agreements" are also probably outside of the scope of a computer incident. For these reasons, a Finance/Administration section will probably not be established during a computer incident.

Incident Action Plan

The Incident Action Plan, as described briefly above, is the blueprint for attacking the incident. It's generated by the planning section, other section chiefs give input, and the Incident Commander then approves it. Once that plan is approved, the Operations section executes it.

One consideration that is different between computer incidents and many more traditional incidents is that the operational periods involved in a computer incident will be generally shorter than in a traditional incident. It would be absurd to handle an ongoing DoS attack with an operational period of 24 hours, but that sort of operational period is routine for some sorts of extended incidents.

The need to always have an up-to-date Incident Action Plan is the largest factor requiring compression of operational periods. While computer incident response personnel may become mentally fatigued at about the same rate as emergency services personnel become physically exhausted, computer incident responders tend to be more used to working around the clock than responders in outdoor incidents where daylight is a factor. In those sorts of incidents, the planning section team members may debrief the responders and then work late into the night or morning setting goals for the following day's events.[5] In a computer incident, the planning and intelligence gathering functions must be an ongoing effort. Perhaps an operational cycle (and hence, an Incident Action Plan) will only last 2-4 hours.

Of course, on single operational cycle incidents a written IAP and a formal planning section are often skipped as responders clean up a known problem of a similar type. In this case, verbal instructions from the IC may be sufficient planning. However, an IC must always be open to see that the incident may be escalating in complexity or its scope may have been initially underestimated. In those cases, an IC must be prepared to expand his or her ICS team to cope with the additional planning and coordination duties needed for the expanded incident.

[5] If computer incidents adopted such a day/night cycle, knowing the stereotypical sleeping habits of computer professionals one might wonder if the operational and planning staffs would argue about who got to stay up all night.

© SANS Institute 2000 - 2005 Author retains full rights.

Span of Control

In traditional ICS incidents, the ability to keep track of incident responders in dangerous situations is a prime consideration for enforcing span of control limits within the ranks of the 'operations' section. The other reason, effective command, control, and communication, is more applicable to the non-operational resources in a traditional ICS response, and key for all sections in a computer incident response.

There exists some flexibility within span-of-control about how small teams of individuals can be represented. If an incident response requires a group of people to work together in close proximity, that team can probably be represented on an ICS organizational chart as a single entity with a designated unit leader. If the team is diverse in physical location, it may be prudent to represent the team as a collection of single person resources, reporting to a branch director.

The span of control guidelines within ICS are a tool used to optimize the amount of communication and management going on during a stressful situation. Any IC who chooses to ignore their recommendations risks a communication breakdown during an incident.

Future Directions

This document has been an attempt at mapping the existing methods of the Incident Command System, which has experienced a great deal of success and refinement during the last 15 years, onto the relatively new field of computer incident handling. Many of these ideas have not been field tested; before the success or failure of this concept can be demonstrated, computer incident responders will have to try to use these guidelines to create their own ICS response organization. Perhaps in 2001 there will be sufficient experience to confirm or repudiate the suggestions set forth here. As citizens and governments realize the critical role that information technology infrastructure plays in their daily lives and operation, a call to formalize and document computer incident response methodologies will certainly arise. It is the author's sincere hope that this effort will prove to have been a significant contribution towards that end.

About the Author:

Jonathan Clemens, CISSP, commands a 60-person Emergency Response Team at Intel's DuPont, Washington campus. He received advanced ICS training from the U.S. Coast Guard, and teaches ICS as a member of the U.S. Coast Guard Auxiliary. He has been working in computer support and administration for twelve years, and currently is an Information Security Specialist with Intel's Corporate Information Security department. He holds various computer certifications in addition to his CISSP, including CCNA, MCSE, GSEC, and CCP.

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Last Updated: July 25th, 2017

Upcoming Training

Security Awareness Summit & Training 2017	Nashville, TN	Jul 31, 2017 - Aug 09, 2017	Live Event
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Memphis SEC504	Memphis, TN	Aug 21, 2017 - Aug 26, 2017	Community SANS
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Mentor Session AW - SEC504	Milwaukee, WI	Aug 23, 2017 - Sep 29, 2017	Mentor
Mentor Session AW - SEC504	New York, NY	Aug 24, 2017 - Sep 08, 2017	Mentor
Mentor Session - SEC504	Denver, CO	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS vLive - SEC504: Hacker Tools, Techniques, Exploits and Incident Handling	SEC504 - 201709,	Sep 05, 2017 - Oct 12, 2017	vLive
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
SANS Dublin 2017	Dublin, Ireland	Sep 11, 2017 - Sep 16, 2017	Live Event
Mentor AW - SEC504	Santa Clara, CA	Sep 11, 2017 - Sep 22, 2017	Mentor
Mentor Session - SEC504	Arlington, VA	Sep 20, 2017 - Nov 01, 2017	Mentor
SANS SEC504 at Cyber Security Week 2017	The Hague, Netherlands	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Columbia SEC504	Columbia, MD	Sep 25, 2017 - Sep 30, 2017	Community SANS
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
Mentor Session - SEC504	Boston, MA	Sep 26, 2017 - Nov 07, 2017	Mentor
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Mentor Session AW - SEC504	Houston, TX	Oct 02, 2017 - Dec 11, 2017	Mentor
Mentor Session - SEC504	Columbia, SC	Oct 03, 2017 - Nov 14, 2017	Mentor
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
Community SANS Chicago SEC504	Chicago, IL	Oct 09, 2017 - Oct 14, 2017	Community SANS
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event