Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Computer Incident Response Team

No matter how well your network is protected, eventually there will be an incident that you are not prepared to handle by yourself. It could be because the problem is beyond your technical capabilities, or it could be because you have not been empowered to make the necessary decisions or to take the necessary actions. Does you're company have a plan for this contingency? No company's security policy should be considered complete until procedures are put into place that allow for the handling and recovery from even the ...

Copyright SANS Institute
Author Retains Full Rights

AD

Computer Incident Response Team

GIAC Certification Version 1.2F

Michelle Borodkin

You are a trained computer security specialist. You have kept up to date with the latest security holes and patches for your software and operating systems. Your logs are in order and reviewed regularly. Your firewall and intrusion detection system are fine tuned, just the way you like them. You're ready for anything… Right???

No matter how well your network is protected, eventually there will be an incident that you are not prepared to handle by yourself. It could be because the problem is beyond your technical capabilities, or it could be because you have not been empowered to make the necessary decisions or to take the necessary actions. Does you're company have a plan for this contingency?

No company's security policy should be considered complete until procedures are put into place that allow for the handling and recovery from even the most devastating of incidents. One possible solution is the inclusion a Computer Incident Response Team (CIRT) within the company's incident response procedures.

This paper is designed to answer the big questions about Computer Incident Response Teams including:

What is a CIRT?

Who should be on a CIRT and what function will they serve?

And, What steps need to be taken to implement a CIRT?

What is a Computer Incident Response Team? (CIRT)

A CIRT is 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. It is usually comprised of members from within the company. They must be people that can drop what they're doing[2] (or re-delegate their duties) and have the authority to make decisions and take actions[3].

Who belongs on a CIRT?

Who is included in a CIRT and what they do depends largely on the needs and resources of the company[7]. Below is a list of possible members, why they should be included in a CIRT, and the roles they would likely have to play.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Management

It is essential to have a member of upper level management on the team[2]. Not only do you need someone that can make the big decisions, but without management's support, the team will likely never be an effective resource. Management should be involved in the entire security process including: evaluating security, selecting a team, developing a policy, exercising the plan, and handling incident responces[2].

Management's role during an incident, apart from giving the team the authority they need to operate, is to make the big decisions based on input from of the other members of the team[4].

Information Security

The members of the Information Security team are the employees who are trained in the area of handling electronic incidents. They are valuable assets not only because of the ability to handle a multitude of incidents, but for their ability to provide options and implications of these options to management and other members of the team.

Information Security's role includes assessing the extent of the damage, containment, basic forensics, and recovery.

IT / MIS[4]

Many companies have a separate security and IT department. Their responsibility is to care for the company's data. In the even of an incident, the IT team will need to know where the data can be accessed, and what areas of the network are off limits. If you don't include you're IT members in the loop, you may find your evidence over written by a well meaning tech who discovered a corrupt database and replaced it from a back up.

The IT/MIS roll is to ease the effects to system end users, and to assist the Information Security team with technical matters as required.

IT Auditor[1]

Many companies are beginning to utilize auditors that are specially trained in the area of computer technology. It is their role within the company to be sure procedures are being followed, and to help foster change when current procedures are no longer appropriate. They will more than likely be present during a crisis, but not take a great deal of action at that time.

The IT Auditor's role is to observe, learn why the incident came to be, ensure procedures are being followed, and work with IT/security to avoid problems in the future. They are invaluable members of the team when conducting post-incident reviews.

Security[1]

This refers to the people who are responsible for physical security. If you're faced with an incident that involves direct contact with your system, the security team is the one with the training to assist in this area.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

The Security's role may include assessment of any physical damage, investigation of physical evidence, and guarding evidence during a forensics investigation to maintain a chain of evidence.

Attorney[1]
An attorney is useful for supplying a CIRT with legal advice.
The Attorney's role is to ensure the usability of any evidence collected during an investigation in the event that the company chooses to take legal action.
An attorney can also provide advice regarding liability issues in the event that and incident affects customers, venders, and/or the general public.

Human Resource[1]
Many incidents involve company employees.
The Human Resource's role is to provide advice as to how best to handle situations involving employees. HR will generally not be called upon to assist with an incident until after an investigation has begun, and only in the event that an employee is discovered to be involved.

Public Relations[1]
A company's image is an asset of considerable vale, especially if the company is publicly traded. When possible, most companies like to keep minor incidents quiet and out of the media. Sometimes this isn't an option. If you do have to share information, this is the person that can best advise you as to the message that should emanate from the company, and the best way to propagate that message.
The Public Relations' role is to communicate with team leaders, ensuring an accurate understanding of the issue and the company's status, and to communicate with the press and/or informing the stockholders of the current situation.

Financial Auditor[1]
One of the hardest things to do when an incident occurs is to put a monetary figure on the damage that has occurred as a result of an incident. A monetary value however, is frequently required for insurance companies. An accurate figure will also be needed in the event you choose to press charges under the National Information Infrastructure Protection Act; It is required that you be able to document at least five thousand dollars worth of damage[5].

In addition to these members, you may also choose to include team members from outside your company. These could include but are not limited to professionals such as law enforcement, vendors[4], and/or technical specialist[2].

Your company does not necessarily require that there be one person designated for each of the listed categories. As mentioned above, each company is going to pull together a team based on its needs and available resources[7]. It is however

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

important to ensure that there is someone designated to oversee the needs that may arise for any contingency.

What steps need to be taken to implement a CIRT?

Knowing what a CIRT is, who belongs on a CERT, and what they would do is useful information, but that's just a start. The process of creating and successfully implementing a team begins with planning and the writing of procedures.

If you don't already have incident response procedures that call upon a CIRT, it's time to consider a procedural rewrite. (Remember, you're supposed to be reviewing you're security procedures every six months anyway.)

But, before you start rewriting all you're procedures, it is important to get support from management. Without their support, the team is not assured adequate funding or authorty[2] and the chances for success are greatly diminished.
Some managers choose not to create a team, but to outsource professionals when the time arrives[6]. There are advantages and disadvantages to this method, which are beyond the scope of this paper.
It would be a waist of you're time to create a plan, and then discover that management has other plans in mind. And if you're company has no designs on securing their systems what so ever, you have a long road ahead of you before you approach anyone with a plan to create a whole team to support a nonexistent security procedure.

Once you have discussed with management the feasibility of having a CIRT within your company and the resources he/she is willing do devote to it, the process begins when you create or revise you're current security procedures.

One of the first things you will need to establish is what exactly constitutes an incident[2], and at what point should the team be called in[3]? Assembling the CIRT too frequently over minor issues will slow down reaction time. (Think of the story The Boy Who Called Wolf.) Likewise, you don't want to underutilize you're team. They exist for a purpose: to protect the company's best interest, and yours. Making the decision to take down the company's web server on your own, even if it is in the company's best interest, may leave you on the wrong side of the next computer investigation. Striking a balance, and documenting that line as clearly as possible is essential[3].

The next thing you will want to establish is the process to call the team together. A commonly used procedure is to choose a team leader and contact that person first. The leader then, after assessing the situation, contacts the required members of the team. Unrequired and unaffected team members should not be contacted. During the initial containment period, it is generally preferable to contact as few people as is required[7].

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

In order to call in the Computer Incident Response Team, a list of names and methods for contacting members during both work and non-work hours should be available to all members in the team. The method of contact should include at least one non-email method. If there is an attacker in you're system, you don't want to alert him to your investigation. If there is a natural disaster, you may not have the use of computers at all.

Once incident response, incident handling, and incident follow up procedures have been written or revised, an initial meeting with the members of the Computer Incident Response Team should be held[2]. Every team member should comprehend the importance of their inclusion in the team, and their need to respond quickly when called upon. The team members should understand the type of situations that they will be facing when they are called upon and what duties they are expected to perform when they arrive. This information should not only be explained to the team fully, but should also be included in writing within the incident response procedures.

When all members have been trained, and know what is expected of them, a drill should be scheduled. Create a scenario that will require you to call upon all members in the team. Set it up to be as realistic as possible without actually causing harm to any systems or data. Be sure to include documenting procedures during the practice incident, and an incident review meeting at the conclusion.

This practice has two main purposes. One is to prepare the team so that they can better understand their roles within the group[4]. The other is to discover any holes in the procedures[2]. Don't be surprised if all does not go smoothly. Just record areas that provided difficulties and continue with the practice until you reach the conclusion where the company has fully recovered form you're incident.

After the practice incident, it is important to meet and review the exercise. This is the time to fine-tune you're procedures before making them official. You want your procedures to be as complete as possible, because next time you gather the CIRT, it may not be for a drill.

With luck, you won't need to call upon the CIRT very often. Whether incidents come up frequently or not at all, you want to conduct a practice exercise every six months[2]. If you don't have frequent incidents, it is an opportunity to keep the teams skills sharp. If you do have frequent incidents, it gives you an opportunity to reevaluate the process when reviewing you company's incident response procedures.

Creating a Computer Incident Response Team is not going to be the best solution for every company, but in many if not most settings, it can be an invaluable tool. It will improve response time to any computer base problems you may encounter, ensure that the incident handling methods are supported by

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

the company, and prevent a state of chaos and panic when an actual incident occurs.

1. Ono, Robert "Computer Incident Response Teams" 2000
URL: http://www.caworld.com/proceedings/2000/security_mgmt/ya014pn/

2. Neely, DeQuendre "You've Been Hacked, Now What?" 2000
URL: http://www.securitymanagement.com/library/000797.html

3. Miora, Michael, and Cobb, Stephen "Springing Into Action" 1998
URLl: http://www.infosecuritymag.com/articles/1998/mayspringing.shtml

4. Detecting Intruders -- MPRM Group Limited - Network Security
URL: http://www.mobrien.com/intruders.shtml

5. Frontline: hackers: who's responsible?: computer crime laws
URL:
http://www.pbs.org/wgbh/pages/frontline/shows/hackers/blame/crimelaws.html

6. Lunn, Dorothy "Computer Ferensics – An Overview" 2001
URL: http://www.sans.org/infosecFAQ/incident/forensics.htm

7. Malisow, Ben "Moment's Notice: The Immediate Steps of Incident Handling" 2000
URL: http://www.securityfocus.com/focus/ih/articles/moments.html

© SANS Institute 2001, Author retains full rights

Last Updated: June 19th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**