



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.

### Implementing a Computer Incident Response Team in a Smaller, Limited Resource Organizational Setting

Information security risks are an ever-increasing threat; protecting your organization's information in today's environment is of great concern and importance and it presents a formidable task for organizations to undertake. Many organizations have established Security Programs and Plans to deal with the myriad of threats present for any infrastructure. Security Programs are essential to an organization and aid in protecting you from potential threats and vulnerabilities. However, Security Programs alone will not prote...

Copyright SANS Institute  
Author Retains Full Rights

AD

An advertisement banner for Watchfire. On the left, there is a graphic of a globe and a login form with fields for "log" and "password". The text "YZEIF I" is visible in the background. In the center, a dark blue box contains the text "Testing Web applications for vulnerabilities?". On the right, the Watchfire logo (a red flame) and the word "watchfire" are displayed.

Testing Web applications for vulnerabilities?

# Implementing a Computer Incident Response Team in a Smaller, Limited Resource Organizational Setting

Mary (Missy) Hall

March 15, 2003

GSEC - Version 1.4b Option 1

## Abstract

Information security risks are an ever-increasing threat today given the fact that the number of technically well informed users continues to grow, as well as the availability of the Internet on nearly every desktop. Protecting your organization's information in today's environment becomes a greater concern and importance and presents a formidable task for organizations to undertake. In response to the growing number of threats and intrusion activities, most organizations have established Security Programs and Plans to deal with the myriad of threats present for any infrastructure. Security Programs are essential to an organization and aid in protecting you from potential threats and vulnerabilities. However, Security Programs alone will not protect you and your organization from all incidents, nor will they cover the issues surrounding response to an incident. Many organizations are looking toward developing their own Computer Incident Response Team (CIRT) or possibly outsourcing in this area. A CIRT provide an organization with a structured, clearly defined plan for dealing with threats and incidents. <sup>1</sup>

Smaller scale organizations or those with limited resources have a tendency to think that a Computer Incident Response Team is not necessary or that it is not feasible given their size or fiscal status. It is the intent of this study to focus on and discuss the challenges a smaller organization faces in the implementation of a Computer Incident Response Team. Further focus will be geared toward a simple, practical approach to implementing a CIRT and outlining some of the basic steps involved in the implementation process given the constraints of the organization operating with limited resources.

## Management Buy-in

No matter what type of program, plan or team you are developing within any organization, management support plays an essential role. Obtaining the approval of top-level management or the CEO is an imperative factor in the ability to form and implement an effective CIRT. Management support will provide the key resources in the development of the team, such as personnel, time and funding. Support from top-level management will further aid you in eliciting the participation of various department managers and their staff in developing and forming the CIRT. <sup>2</sup>

Providing justification for a Computer Incident Response Team to management in a smaller environment is not necessarily an easy task. In some cases management is not tech friendly or savvy and therefore may not fully comprehend the need for a “team” to handle “perceived threats.” In today’s economy, many organizations are extremely budget conscious and feel that a formal team is not a viable expense. Some methods to counter and deal with roadblocks at the management level are presented below.

#### Why does our organization need a Computer Incident Response Team?

Management may point out that the organization already has an IT Department that handles all the information systems and security and we have a Security Program in place to cover threats. To counter this attitude, inform management that a coordinated team would serve to further bolster the existing Security Program within the organization and that the CIRT would be aligned with organization’s Security Program. Without such a team in place, if an incident were to occur, how would it be handled within the organization, who would coordinate these efforts and ultimately be responsible for following through with incident resolution and return to business. A CIRT would serve to provide the organization with an organized and speedy response in the case of threats and would assure a more rapid return to business after an incident. Approaching this from a fiscal standpoint, which would be more costly to an organization, implementing the CIRT or having your systems off line for a day or two, possibly a week, because of a hacker? Failure to respond to incidents quickly and efficiently can be very costly to the organization.

We do not have the financial or personnel resources available to form a Computer Incident Response Team. A barrier of this type can be dealt with using several different approaches. One approach would be in looking within the organization for your personnel resources. A team does not have a specified number of members, perhaps a handful of skilled individuals. Within a smaller organization, this team may consist of key individuals from varied departments. An example of these personnel could include the CIO, IT department staff, help desk staff, security staff, risk manager and/or human resource staff. These team members in most cases can be utilized for the Incident Response Team without re-organization or with minor re-alignment of responsibilities. By using existing personnel within the organization, you may be able to form an effective CIRT without employing new personnel.

One method of establishing an effective CIRT with limited resources is to utilize what the organization currently has in place. Look to your organization’s Disaster Recovery Program for membership for the CIRT. Members of the Disaster Recovery Team could be recruited to serve on the CIRT with some additional training.

Once you have obtained management support for the development of a team, you are ready to begin the basic steps needed to form and implement the team.

The steps provided are a general guideline for organizations with limited resources and may need adjustment according to your company's particular size or circumstance. These steps do not necessarily need to be completed in the order listed and may be performed simultaneously.

### Select Team Members – Define Roles and Responsibilities.

When selecting team members keep in mind that team size is not the most important factor. The most important aspect of the team is to ensure that you have a group that can focus on the particular needs of your organization, work within a team setting and possess interpersonal skills. A CIRT can consist of core members and additional support team members, consisting of individuals with specific areas of expertise and skills, which can be called upon during incident handling, if needed.<sup>3</sup>

A few of important considerations for CIRT membership are:

- Team Leader – core team member
- IT Staff – core team member
- Security Staff (Information and Physical) – core team member
- Risk Manager – core team member
- Disaster Recovery Team - support team member
- Legal – support team member
- CFO or Financial Auditor – support team member
- Human Resources – support team member

Once membership selection is completed, each member's responsibilities or role within the team should be clearly defined. Clear definition of responsibilities is essential to ensuring that there is no confusion during the handling of incidents. Written responsibilities are ideal, however, this is not always possible if team members' primary responsibilities fall within another department in your organization.

### Develop a Mission Statement.

Any team within an organization must have a mission statement that clearly states to the constituency the team's core activities, goals and their level of authority within the organizational structure. In the area of a CIRT, the mission statement is especially important because the nature of a CIRT may be at times intrusive to the constituency it serves. A mission statement, which clearly outlines the CIRT's purpose and authority, can be a valuable aid in dealing with your constituency during the incident handling process. In developing the mission statement, you should be knowledgeable in the areas of the organization's existing strategic plan, policies and standards of practice. The mission statement should be in alignment with the organization's security program and policies and approved by management.<sup>4</sup>

## Determine Incident Response Needs.

Unless you know your organization from the top down, making a list of all possible service needs would be an insurmountable task. An assessment of your organization's incident response needs should be conducted to serve as a starting point in identifying incidents within the organization as a whole and to aid in developing policies and procedures for the CIRT. <sup>5</sup>

An assessment can be conducted by means of a questionnaire distributed to relevant individuals or the assessment can be performed through an interview and discussion process. Personal experience in conducting needs assessments with various departments throughout my organization has proven to be a difficult task. I have found a greater degree of success can be achieved through the personal approach rather than distributing questionnaires and requesting they be returned by a specified date. I have also found that more information can be gleaned from individuals if they are given the opportunity to ask questions. Another benefit of conducting assessments personally is that you are given the opportunity to share information about the CIRT and begin to get buy in from your constituency. The down side to this method is that it can be very time consuming depending on the size of your organization. An alternative method for conducting the personal assessment is to meet with entire group for a scheduled session and complete the assessment with all parties at one time. Another option in the assessment process is using the CIRT members to help in performing personal assessments, which would also give the team exposure to the constituency.

Individuals that you should include in the assessment interview might include, but are not limited to:

- Department Managers
- IT Staff
- HR Staff
- Help Desk Staff
- Security Staff (Information and Physical)
- Risk Management
- Users
- CIRT's from similar organizations

## Developing Policies, Procedures and Documentation.

"Policies are governing principles adopted by organizations or teams." <sup>6</sup> Policies communicate to the constituency in a clear and concise manner what is expected of them and what the organization's response will be. Developing effective policies within any organization is a lengthy and difficult matter. Entire books have been devoted to this subject alone and it is beyond the scope of this paper to address. It is the intent of this paper to focus on the need for policy development in implementing a successful CIRT.

Policy development plays an essential role in a CIRT in that the policies will provide your constituency with a guideline to follow when a given incident arises. Without policies in place to direct constituents during an incident, even the best CIRT is virtually ineffective. The team may not be able to respond to and handle an incident before the harm or damage has been done to the organization. In the environment with limited resources, call on your team members to assist in the process of policy development. Do not hesitate to research existing resources within your organization. Most organizations have already developed disaster recovery plans/programs, security programs, etc. that can be a useful tool in developing CIRT policies. Existing organizational policies may be able to incorporate the CIRT with a few revisions. Research policies on the Internet, one source of policy templates can be found in RFC 2350: "Expectations for Computer Security Incident Response."<sup>7</sup> Lastly, if your organization has someone whose job is solely policy development, enlist his or her assistance in the development process if possible. If his or her assistance is not possible, ask that they provide you with your organization's guidelines regarding policy development and ask for their assistance in reviewing your policies.

Written procedures are a critical element for a successful CIRT. Procedures should be written that clearly state what steps and actions are to be taken in a particular incident. Procedures should be written to cover those areas identified by the CIRT's needs assessment. All team members should receive training and should be kept abreast of all incident handling procedures, however, it is unlikely that all members will be able to recall all the steps involved in a particular procedure. Therefore, it is a good practice to create a CIRT Operations Manual or Guide. The Operations Guide contains all operational procedures and may contain other documents and information relevant to incident handling.<sup>8</sup>

Other relevant information that may be contained in the Operations Guide:

- Contact Information (team members, investigative agencies, vendors, federal reporting agencies, etc.)
- Incident report forms (internal and external)
- Administrative report forms
- Equipment list
- Checklists

The Operations Guide will need to be readily available to all team members, especially during incident handling. Publish a copy on the organization's Intranet site (available to CIRT members only), as well as maintaining hard copies with a few of the core team members. The Operations Guide should be reviewed and updated on a regular basis. This may sound like a monumental task, but if you look within your organization, you may find procedures already developed that may meet your needs with minor adjustments. Contact other CIRTs to see if they will share what procedures have worked for them and research the Internet for sample procedures.

## Communications.

Communications play a vital role in implementing a successful CIRT. A CIRT needs to stay in touch with its constituency on a regular basis to affect a centralized reporting function and to share important information with the organization.<sup>8</sup> Further, communication between the users and the CIRT helps to ensure the organization's awareness of the CIRT's role with the organizational structure and will help the team gain buy in at all levels. I cannot stress enough that two-way communications must exist for the CIRT to survive. In an organizational setting where the CIRT also has other roles, it is all too easy to get overwhelmed with your regular responsibilities and let the lines of communication dwindle. It is necessary that you keep these two-way conversations open and functional. In many cases the users may be our first alert that an event or incident has occurred. If the communication lines are down, how will the constituency alert the CIRT? Chances are they will ignore the event and wait for the CIRT to address the event first.

Another important factor in the area of communication is the CIRT's responsibility to keep all users up to date on alerts, vulnerabilities, threats and the expected methods of response. Again, it is very easy to get caught up in your regular duties and forget to notify the constituency that there is a new virus circulating and they need to update their virus protection. Lines of communication should be clearly defined within the CIRT as to which team member is responsible for communicating information to the constituency, how this communication will be achieved and when this is to be completed. There are a number of methods to communicate with your constituency, but this paper will concentrate on just a few of them.

E-mail is a very effective tool for reaching your constituency quickly and efficiently. Setting up a mail group or distribution list is the first step. Be sure to keep your list current with staff changes within the organization. When the team receives new information concerning threats or vulnerabilities, e-mail will be one of the quickest avenues in disseminating this information. When sending information to the users make certain to include clear instructions regarding any steps they may have to take in relation to the information communicated. For example, applying the latest service pack or updating a .dat file.

Bulletins/notices can be another effective method of communication. Posting notifications and instructions on the organization's Intranet site has two benefits, new alerts are readily available and the Intranet site could serve as a repository for previous alerts, notifications and security information. The Intranet site can also include your policies, team member contact information, reporting guidelines and an electronic incident report form. Consider, also, having a paper bulletin board in a strategic location for the constituency that may not have access to the

organization's Intranet site. The paper bulletin board will also serve as a backup location in the event your network is non-functional.

Communication between team members is another important factor to consider. These communication lines should remain open during normal operations, but more importantly during incident handling. Establish contingency methods of communication in the event that normal communications channels fail or are not secure. The contingency communication methods could be included in your CIRT Operations Guide.

### Training.

This paper will touch lightly on the topic of training. Exploring training issues would be too lengthy to address here. We all know the benefits and importance of training especially given the constant changes in today's technology. Education and training is important not only in the case of team members but is a major consideration for your users at all levels. Users can be a major source of security breaches if they are not knowledgeable concerning security policy and acceptable computer/network usage.

Training and education should occur constantly throughout the users' employment with the organization. The training process should begin during the employees' initial orientation phase and continue during their job specific training (especially when duties include usage of the organization's network). Education should also continue throughout the user employment in the form of alerts, notifications, policy updates or additions and in-service or on-the-job training. If your organizational policies include annual reviews/training, it would be advantageous to include the role and responsibilities of the CIRT in the annual review process, as well as a review of the CIRT's policies.

The importance of training and education for the team members goes without saying. For the purposes of this paper, I will only touch briefly on the important factors involved in team member training. In short, in the limited resource environment, it is not always financially feasible to send the entire team for training. Consider sending one team member to relevant training opportunities with the understanding that this information is to be presented to the entire team. Another source of education exists for team members in the form of journals and papers, which are readily available on the Internet free. Consider purchasing books, which can also, serve as a resource for the entire team. Check with other departments within your organization for resource material, such as the risk manager or security. Utilize web sites to stay abreast of new threats and vulnerabilities and approaches to combating and dealing with these. Establish contact with CIRTs from other organizations and exchange information, knowledge and experience. Find out what incidents they have faced and what procedures have worked for them in handling the incident. As you can see, there

are a number of different ways you can help maintain the proficiency level of the team without a large expenditure.<sup>9</sup>

If the CIRT consists of existing staff members and they participated in the other phases of the team development, such as policy and procedure development, then they will not need training in those areas. If, however, you have to hire staff for the CIRT, you will have to design a training program for these individuals. This program should include the team's policies and procedures, roles and responsibilities, as well as training regarding your constituency; this of course, is in addition to the organization's training programs. Most importantly, all CIRT members, whether new staff or those recruited from within the organization, receive in depth training in proper incident handling techniques as defined by your organization.

#### Tracking and Reporting System.

In order to ensure a successful team you need to have a reporting mechanism in place to communicate your activities to management. If management is unaware of activities of the team, the team could lose credibility or, in the worst-case scenario, be doomed to failure. To help in the reporting function, a tracking mechanism should be established to document the team's activities during incident handling and further document the outcomes. The tracking mechanism you develop should take into consideration the information gleaned from the needs assessment conducted with the constituency, your organization's security program and the CIRT's policies. Further information included in the tracking system would be the incident type; who, what, when, where and why the incident occurred; how it occurred and what was the resolution in the case. When it comes time to report your activities to management, be it monthly, quarterly or annually, the team can simply retrieve the data from the tracking system.<sup>10</sup>

Another consideration in the area of reporting is whether the incident should be reported outside the organization to law enforcement or government agencies. Before reporting any incident further than the organizational level make certain you know what your organization's policy states, as well as local laws and statutes. Further information regarding incident reporting can be found at the CERT Coordination Center [www.cert.org](http://www.cert.org).<sup>11</sup> Other links for reporting include The Federal Computer Incident Response Center, [www.fedcirc.gov](http://www.fedcirc.gov) and The National Infrastructure Protection Center [www.nipcc.gov](http://www.nipcc.gov).

#### Lessons Learned.

After the resolution of an incident, the team should examine all information regarding the incident handling process and the resolution. The data gathered from the review process would be a valuable tool for the team's further development. This information will aid in identifying strengths and weakness and

help clarify where you may need further training, skills, manpower, policies or procedure revisions. <sup>12</sup>

The review process should include, but is not limited to the following:

- Did procedures work?
- Do additional procedures need to be developed?
- Did the checklists aid in your handling process?
- Do checklists need revision or new ones developed?
- Were policies in place to aid in smooth handling of incident?
- Would further training benefit the team or the constituency?
- Did communications channels work in the response process?

The data gathered during the review process will also guide you in the area of policy and procedure development and revisions. Keep in mind that as information technology advances, so do the threats of intrusion, which will be the driving force in the further evolution of the CIRT.

Summary.

Development and implementation of a Computer Incident Response Team is a major undertaking in any organization. The process, no matter how simply you approach it, requires a significant amount of time and dedication. I believe, however, the benefits far outweigh the consequences; one incident, without rapid response can be costly to your organization. A CIRT may not be necessary for every organization. In some cases, costs of developing and maintaining a team may outweigh the cost of the possible damage. In any case, your organization's size, business type, resources and circumstances will be the determining factor in your decision to implement a team or not.

© SANS Institute  
Author retains full rights

- 
- <sup>1</sup> META Security Group. "Developing a Security Incident Response Team" 2002. <http://www.metasecuritygroup.com/library/whitepapers/DevelopingASecurityIncidentResponseTeam.pdf> (13 March 2003).
  - <sup>2</sup> Martinez, Simon. "Federal Government Incident Response Team (IRT)." Version 1.0. April 23,2002. [http://secinf.net/misc/Federal\\_Government\\_Incident\\_Response\\_Team\\_IRT.html](http://secinf.net/misc/Federal_Government_Incident_Response_Team_IRT.html) (11 March 2003).
  - <sup>3</sup> Sandra International Corp. "Sample Standard Practice for Implementation and management of a Computer Incident Response Team (CIRT)." © 1998. [http://www.securityunit.com/pubs/cirt\\_std.doc](http://www.securityunit.com/pubs/cirt_std.doc) (9 March 2003).
  - <sup>4</sup> Miora, Michael. "White Paper: Building an Incident Response Team" November 14, 2002. <http://www.contingenz.com/Building%20an%20IRT.pdf> (11 March 2003).
  - <sup>5</sup> Carnegie Mellon Cert Coordination Center. "Creating a Computer Security Incident Response Team: A Process for Getting Started" <http://www.cert.org/csirts/Creating-A-CSIRT.html> (12 March 2003).
  - <sup>6</sup> West-Brown, Moira; Stikvoort, Don; Kossakowski, Klaus-Peter. "Handbook for Computer Security Incident Response Teams (CSIRTs)" December, 1998. <http://www.sei.cmu.edu/pub/documents/98.reports/pdf/98hb001.pdf> Carnegie Mellon Software Engineering Institute (9 March 2003).
  - <sup>7</sup> RFC 2350: "Expectations for Computer Security Incident Response" Networking Group, June, 1998. <http://www.ietf.org/rfc/rfc2350.txt> (9 March 2003).
  - <sup>8</sup> Wack, John P. "Establishing a Computer Incident Response Capability (CSIRC)" NIST Special Publications. November, 1991. <http://www.securityunit.com/pubs/800-3.pdf> (9 March 2003).
  - <sup>9</sup> Smtih, Danny. "Australian Computer Emergency Response Team" The University of Queensland. January 1, 1995. <http://www.auscert.org.au/render.html?it=2252&cid=1920> (9 March 2003)
  - <sup>10</sup> Miora, Michael. "White Paper: Building an Incident Response Team" November 14, 2002. <http://www.contingenz.com/Building%20an%20IRT.pdf> (11 March 2003).
  - <sup>11</sup> CERT® Coordination Center. "Incident Reporting Guidelines" [http://www.cert.org/tech\\_tips/incident\\_reporting.html](http://www.cert.org/tech_tips/incident_reporting.html) (15 March 2003)

---

<sup>12</sup> U.S. Department of Transportation. "Departmental Guide to Incident Handling Planning" DOT H 1350.255. <http://www.securityunit.com/pubs/incitrans.htm> (11 March 2003).

© SANS Institute 2003, Author retains full rights



# Upcoming SANS Training

[Click Here for a full list of all Upcoming SANS Events by Location](#)

SANS San Francisco 2009	San Francisco, CA	Nov 09, 2009 - Nov 14, 2009	Live Event
Hong Kong Advanced Forensics Seminar	Hong Kong, Hong Kong	Nov 09, 2009 - Nov 14, 2009	Live Event
SANS Vancouver 2009	Vancouver,	Nov 14, 2009 - Nov 19, 2009	Live Event
SecurityByte 2009	New Delhi, India	Nov 17, 2009 - Nov 20, 2009	Live Event
SANS Geneva CISSP at HEG 2009 Autumn	Geneva, Switzerland	Nov 23, 2009 - Nov 28, 2009	Live Event
SANS London 2009	London, United Kingdom	Nov 28, 2009 - Dec 06, 2009	Live Event
SANS WhatWorks in Incident Detection Summit 2009	Washington, DC	Dec 09, 2009 - Dec 10, 2009	Live Event
SANS CDI East 2009	Washington, DC	Dec 11, 2009 - Dec 18, 2009	Live Event
SANS WhatWorks in Data Leakage Prevention and Encryption Summit 2010	New Orleans, LA	Jan 07, 2010 - Jan 12, 2010	Live Event
SANS Security East 2010	New Orleans, LA	Jan 10, 2010 - Jan 18, 2010	Live Event
SANS AppSec 2010 and WhatWorks in AppSec Summit	San Francisco, CA	Jan 29, 2010 - Feb 05, 2010	Live Event
SANS Sydney 2009	OnlineAustralia	Nov 09, 2009 - Nov 14, 2009	Live Event
SANS OnDemand	Books & MP3s Only	Anytime	Self Paced