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

Outline of a

Computer Incident Response Team Charter

'Moving through the first few steps towards establishment of a CIRT in a large disperse Federal Government Organization'

James G. McCallum

GIAC Security Essentials Certification (GSEC)

Practical Assignment
Version 1.4b
(Amended August 29, 2002)
Option 2
Case Study in Information Security

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Abstract/Summary

This work discusses a process for establishment of a Computer Incident Response Team (CIRT), with concentration on the development of a CIRT Charter. It begins with a description of the overall organization, discussing a view of the organizational history and how Information Management and computer security evolved. Formation of a malware response team into the existing computer support structure is discussed along with the realization of a more comprehensive CIRT need. The CIRT charter is discussed with steps from; 1) build management support through development of a mission statement, 2) identification of core services or goals for team responsibilities, 3) develop formal team structure, responsibilities and skills necessary for a core team, 4) recognition of cycling of core team membership with the incorporation of a distributed peripheral team, and 5) identify skills needed to meet all team goals. The paper concludes with a discussion and recommendations for the next steps to CIRT establishment. Throughout the paper citations are included to assist the reader in gaining more complete knowledge. The process of establishing a CIRT should not be taken lightly. This work clarifies the need to gain support along the road and finishes with next steps.

In the Beginning

Before you can grasp the complexity of this undertaking and conceptualize how it may fit into your situation, it is necessary to discuss the history of our agency Information Resources Management (IRM) organization, its evolution and adaptations to the overall organizational situation.

We are a relatively large Federal land management agency with many thousand employees, geographically distributed throughout the entire United States. The agency has historically, been dispersed with a central Washington DC Headquarters Office. The DC office is responsible for oversight and policy but impacted the distributed field locations as little as possible. The US was divided into regional offices, which maintained oversight and management over their geographical responsibilities. As a land management agency, the work is done at the lowest level of the organization. A vast majority of the employees spend most of their time completing fieldwork and returning to the office when necessary for paper work and general employment requirements, like reporting time worked. Coordination between various units is seldom required and independence is the hallmark of the organization. The general oversight that management employs encourages a “can do” attitude where everyone is encouraged and expected to be self-sufficient, capable of dealing with any situation efficiently without assistance, intervention, or direction.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The implementation of computers into the agency has been a relatively new and gradual process. The IRM organization in general was carved out of the overall employee population and evolved along a similar path as the organization, dispersed and independent. The wide-area network incorporated into the office automation platform required some centralization of effort and was implemented at a regional level with local support. General standards were incorporated for the networks at an early stage but enforcement was impossible. The office automation platform included minicomputer system with x-terminals for users. A standard image was established and supported nationally, but local modifications were necessary and common practice across the agency. Enforcement of a national standard image was nonexistent. Even when standards were adopted, they were rarely distributed and seemed to be arbitrary and hampered productivity. *Therefore standards were unenforceable!* The one policy that was enforced was non-implementation of personal computers (PCs). PCs sprang up in the background, unsupported, uncoordinated and ignored. The complexity of implementation and management of PCs was just not something management would accept until it was inevitable!

The implementation of a client/server environment, with PCs and UNIX file sharing, was forced on the organization by the *users* recognition of the advantage and usefulness of the tool. PCs are now supported as an agency requirement. The agency could not function or compete without them, at this point. The computer support staff has been minimally supported due to the "can do" attitude of management and the general population, along with budget constraints continuously griping federal organizations. The client/server environment put the agency on the road to a computer productivity gain that has been recognized in the agency as positive and long overdue. It also integrated a platform that is inherently insecure! In its effort towards security enhancement, national implementation included Open Systems Foundation's DCE/DFS for file system security on the UNIX platform, making operational overhead complex and often bypassed for the sake of productivity. The windows platform has migrated to a more secure template. This move disabled many of the functions users took for granted in the past, causing user frustration. A solution was developed which allows computer support to temporarily enable the functions. This has increased the responsibilities of the IRM community and invoked bypassing of the security functions.

The IRM organizations matured in this dispersed and fiercely independent atmosphere. Employees implemented PCs into the organization in the same spirit of individual responsibility the agency reflected organizationally. Employees took ownership and made it work the way they wanted. If a control impeded their productivity the reaction was to identify a work around and implement it. The security implementations of IRM were seen as inconveniences to be removed. The local IRM organizations are autonomous and have minimal oversight. In many cases the local employees encourage IRM to identify ways to bypass security precautions. And, in an agency the size of ours control became

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

impossible. There is little incentive from DC to train employees in proper computer usage because the productive work of the organization is done on the land not in the office. The IRM community in general is overworked and underpaid with little influence to improve the situation.

The integration of an IRM security organization was much the same as PCs. The national Security Officer position sat vacant for 3 years. Field level Security Officers at the regional centers took on the responsibility for official policy creation and upward reporting, with the full load of local issues. We had a single part time security contractor in an outlying location responsible for generating reports on computer security of the agency as the requests arose. There were requirements from outside the organization that remained unacknowledged or tentatively responded to with, "we are working on it." Computer security training of the general employee population was left to local sites. Education of the population, and even other IRM organizational units, was sparse and often overlooked due to understaffing. Commonly, the Security Officer was the systems operator and involved with network functionality. The three responsibilities conflict with each other.

An ad-hoc incident response organization grew within the IRM community but was unofficial, informal and unrecognized. It was composed of a loose-knit group of individuals having some of the security responsibilities in their regional areas plus the coordinating contractor. This contractor would contact the field Security Officer if issues were identified. The Security Officer and contractor would work the issue out together, and it was the contractor's responsibility for upward reporting of incident recovery. There was no formal policy or procedure for accomplishment and verification.

Over the last year, the organization has made strides towards a more coherent and organizationally viable national IRM service capability. We have implemented a user computer support center for agency-wide support of computer software and hardware needs. It is a single point of contact for any employee to call for computer problems. We have implemented a national database for problem resolution documentation, which is rapidly growing to include all computer user issues. Under this umbrella it became possible to integrate a basic computer security incident response capability. A four-person, ad-hoc group of Security Officers convened to integrate this capability into the support center. Deciding to start small, we began responding to malware issues through this vehicle, creating the Malware Response Team (MRT). MRT added support for desktop anti-virus software to malware. MRT allowed us to identify and track issues that were national in scope, helped us significantly improve upward reporting requirements, and improved incident response time.

My contributions to this group included coordination of the weekly conference calls and instituting collaborative tools to interact during the planning sessions. I invested my time in identifying the items to capture in the malware repository

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

database, which the team established for the computer support center to utilize in their initial response capabilities. The MRT would populate the repository with response procedures for particular virus infections to establish a common policy nation wide. This was the initial step in our organizational push towards a formal computer incident response capability within the agency. It has been extremely successful.

With the recent hiring of a national Security Officer, the recognition of the need for a formal computer incident response team has been gaining needed status. Additional impetus came from our parent agency's distribution of policy mandating the agency to "establish and implement an internal incident response capability."[1] As within all organizations, there are a limited amount of resources to trade between responsibilities. There is little resource growth and an increased competition between the various disciplines for decreasing budgets. In this atmosphere, it is an uphill battle to demonstrate the increasing need for computer security and an independent, recognized computer incident response organization.

Starting the Education Process

Over the past six months I have attempted to educate my IRM team and management on the potential for disastrous security incidents to occur, bringing security concepts to many groups formally and informally. We have explored the threat environment with some success. Educating users through the use of practical examples and passages like this from the National Institute of Standards and Technology (NIST) that;

> "Along with the growth and spread of computer technology, a similar growth has occurred in the ways in which high technology can be exploited for harmful purposes. Four factors have increased the risks of malicious exploitation:
>
> An emphasis on data confidentiality (and not integrity or availability);
> Increased use of local and wide area networks;
> Extensive use of personal computers combined with lack of user training;
> Increased chances of vulnerabilities due to system complexity."[2]

As a member of the MRT, I accepted the responsibility of second level response to support center tickets. I have become the team lead on issues dealing with desktop anti-virus software. Integrating computer security into our environment has been difficult. The seriousness of computer infections is not fully appreciated by the general employee due to lack of education on the potential implications of an outbreak and the speed of spread. From my experience, certain words, when used, can create a change in attitude. Words such as Trojan horse or key capture, will capture user attention and they become very responsive and helpful. The situation is personalized and requires employee involvement. Pop-up messages are annoying and users don't complain unless it is excessive. Overloading of inboxes with Spam, an annoying issue initially, has become accepted as the price of being connected to the Internet. Scams and

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

sexually explicit e-mail is a concern that the employee is willing to invest some time into notification of the security organization.

The MRT concurs that a re-image is the best practice to insure we are maintaining a secure environment. This practice is always the final response to an incident that has the potential of leaving spy-ware or Trojans in its wake. The requirement to reload the PC image is generally fought because of the productivity loss, due to time required by IRM and the user, to reestablish the PC to a useful state. The recognition of the benefits of this best practice, is slowly integrating into the general user population, but will continue to be an issue in our environment. This drastic step must be thoroughly discussed and justified with the user and local computer support before it is accepted and implemented. A national policy to mandate re-image due to serious infection would smooth this process.

Begin Knowledge Growth for CIRT

Additionally, education of the IRM Security community has been improving with the national coordination of annual SANS security training. In the fall Security Officers meeting, a Computer Incident Response Policy Team was created. This was the first official recognition by IRM of the need and willingness to invest resources in a CIRT. I was elected as the lead, in which capacity I have pushed the team to develop products and implementation procedures. I have setup weekly conference calls and coordinated responsibilities of other members of the workgroup. At the kick-off meeting we decided to spend time researching incident response processes and procedures commonly used in the security community. This task was divided, half the members researched on the WWW, and half researched through public libraries and bookstores for reference materials. We located and have utilized two major resources. The first a book *Incident Response*[3] by Kenneth R. van Wyk and Richard Forno, and the second on the WWW, the *Handbook for Computer Security Incident Response Teams*[4] by Moira J. West-Brown, et al. from the CarnegieMellon Software Institute CERT Coordination Center. These two references were used throughout our policy teams CIRT discussions and were extremely helpful, and recommended, for everyone in this beginning implementation phase.

Understanding requirements and needs, as identified in both resources and the SANS Security Essentials course materials, has been beneficial in establishing management acceptance, “buy in”, and support of the need for a computer incident response team (CIRT). Step 1 on the WWW.CERT.Org web site states “experience shows that without management approval and support, creating an effective incident response capability can be extremely difficult and problematic.”[5] Particularly in federal government, management support is understood as critical to the continued functioning of an incident response capability. “Effective incident response in any organization must begin with management. Management is responsible for providing the support, tools, personnel, and

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

financial backing needed to ensure the successful implementation of an IRT."[6] The initial need is the marketing of benefits to a formal, organized CIRT staff. The most effective way we identified to accomplish this, was through education and presentation of a, well-written, CIRT charter that management can review, discuss and adopt with input, establishing ownership.

Getting Down to Business

A charter became the next agenda item for the Computer Incident Response Policy Team. Michael Miroa's white paper, *Building an Incident Response Team,* identifies the "overarching goal of responding to an incident should always be to prevent further damage and to restore functions to normal as expeditiously as possible, consistent with organizational policies. A clear, written mission and charter establishing the team is essential to achieving this goal as well as to the clear presentation of ROI."[7] The first section of our charter, as identified within the *Handbook for Computer Security Incident Response Teams* started with the development of a mission statement. "A mission statement is imperative to establish a service and quality framework, including the nature and range of service provided, the definition of its policies and procedures and the quality of service…The missions statement of every CSIRT must have the backing of senior management in the parent organization. Without such backing the CSIRT will struggle to obtain recognition and resources."[4]

The mission statement development forced discussion among the team as well as with IRM management, but the product is simple, direct and meets all the guidelines. The mission statement incorporated the three traditional security pillars discussed by Bruce Schneier in *Secrets & Lies* confidentiality, integrity and availability: "Confidentiality is not much more than privacy…integrity is every piece of data is as the last authorized modifier left it…availability is about ensuring that an attacker can't prevent legitimate users from having reasonable access to their systems."[8] Our final mission statement became;

> "The Computer Incident Response Team (CIRT) supports the business operations of the Organization through the rapid mitigation of all incidents adversely impacting the confidentiality, integrity and availability of its information infrastructure and assets."

Goals of a Team

The next step in our process was to identify services/goals the team would be responsible for meeting. Danny Smith describes in *Forming an Incident Response Team* that, "Forming an Incident Response Team without a goal is like implementing computer security measures without a policy. If the goal of what needs to be achieved is unclear, then any efforts by the IRT will always be preformed on an "ad-hoc" basis, without a clear picture in mind. This may cause precious team resources to be fruitlessly expended on ventures that yield limited

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

results."[9] There are many resources for identifying these options, a few of which are the *Handbook for Computer Security Incident Response Teams* by Moira J. West-Brown, et al.[4], *Sample Standard Practice for Implementation and management of a Computer Incident Response Team*[10] from Sanda International Corporation, and *Establishing a Computer Security Incident Response Capability* by John P. Wack, NIST Special Publication 800-3. The Wack publication states "goals define the scope and boundaries of the effort, including the type of technology to be protected and the constituency served. Establishing clear and realistic goals will help to determine expectations of the management and the funding necessary."[2]

Our experience, organizational needs, processes and resources guided our selection of services the CIRT would provide. We identified seven unique services the group could provide. We included these in the mission statement as team goals.

> The goal of this team is to ensure maximum operational up time of mission critical IT systems needed by the Organization in its daily operations. This goal is met by (1) awareness training, (2) crisis response, (3) technical services, (4) timely distribution of security notifications, (5) continuous monitoring of potential issues, (6) effective reactions to incidents, and (7) postmortem of every incident. Communications will be maintained in all directions throughout the Organization.

The final core services include; threat announcements, computer incident response, malware analysis and response, incident tracking, collaboration, information dissemination and education.

Team Structure

Once these core services were identified, we moved to the next step of identifying a team structure to meet the requirements of the services. There were minimal guidelines from our parent agency. These guidelines state, the organizations Security Officer will be a standing member of a Core Team. Due to the geographical distribution of the organization, it was necessary to define a Distributed Peripheral Team (DPT) for efficiently reacting to local issues. The CIRT structure was divided between a Core Team component and a DPT component. Recognizing funding would be negligible, expecting a full-time dedicated Core Team, although beneficial, was not likely. Initially, we would propose a Core Team component with members dedicating at least 60% of their time to the CIRT. This structure is similar to the "hybrid" teams identified by Michael Miora, these "hybrid teams generally have a standing core membership comprised of both technical and non-technical members. When a situation arises that must be addressed by the IRT, additional members with specific skills are added to meet the requirements of handling the incident in progress. Once

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

the incident is resolved, the team reverts to its core membership status."[7] I also give credit to *Incident Response*[3] in their discussion of roles and responsibilities discussion. The Computer Incident Response Policy Team identified and agreed upon the following five general positions as necessary for a Core Team;

1) Team Manager,
2) Intrusion Analyst,
3) Incident Handler(s),
4) Security Engineer(s) and
5) Public Advisory Coordinator.

The Team Manager "is responsible for the overall administrative and personnel management of the team."[3] The Intrusion Analyst is responsible for the technical expertise of monitor, identification and verification of an actual intrusion incident. The Incident Handler(s) is "responsible for leading a particular incident response operation or effort."[3] The Security Engineer(s) serves as the technical resource, proposing counter measures for hardening the various platforms supported within the organization. Finally, the Public Advisory Coordinator, as discussed in many publications, must perform the role of determining what information is distributed, when, how and to whom. This position is critical, since "information released to the public should be handled through a single source representing the organization experiencing the incident."[7] This structure with a discussion of roles is included in the team charter.

Recognizing the need for the Core Team members to dedicate a majority of their time to CIRT, we also identified 60%. We felt this will give the members time to gain experience and competence to adequately perform the responsibilities. However, one of the biggest issue facing staffing levels is staff burnout[9]. It is essential to establish the Core Team positions as permanent for continuity yet remain as flexible and as neutral as possible.[6] Integrating a DPT where members are geographically dispersed and represent the organizational distributions of the agency, establishes the flexibility, training opportunities, and a pool of candidates to grow into a revolving Core Team. This integration produces some management friction due to the CIRT not having direct supervisory control over the individuals, requiring a coordinated effort to insure every organization was included. All Directors had to understand and agree with the unfortunate fact of life, that incidents do not occur at a steady rate.[9] Adopting the charter and recognizing that significant time will be required when an incident occurs, needed to be emphasized to Directors. "CSIRT needs to be prepared for the dynamic environment of computer security incident response. A CSIRT needs to be ready to address any situation that may not be explicitly covered by its existing guidelines or expertise."[4] The DPT members will be available, and called upon when necessary, to track local issues and communicate directly with impacted parties. This interaction with the organization was considered critical in forming of the CIRT as well as reacting quickly when an incident occurs. All travel and training expense was recognized as requiring local resources until a fully functioning CIRT could address this issue in more detail.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

One Last Detail - Skills

For the final step, we felt it was necessary to identify skills required to effectively reach all the CIRT goals. In general, they were identified for the Core Team members under the individual positions.

> "Many people incorrectly consider the most important attribute in CSIRT staff to be their technical experience. Although technical experience is a desirable attribute, by far a more critical criterion is an individual's willingness and ability to follow procedures and to provide a professional interface to constituents, customers and other parties interacting with the CSIRT. It is a more desirable approach to hire individuals with less technical experience and good interpersonal and communication skills, and then train them in CSIRT-specific technical skills, than vice versa."[4]

The policy team stressed the requirement for any candidate to have at least the SANS Security Essentials training or equivalent professional course in security awareness. A comprehensive list of skills for team members was found in the *Handbook for Computer Security Incident Response*. Individuals need to have "common sense to make efficient and acceptable decisions whenever there is no clear ruling available and under stress or severe time constraints...effective oral and written communication skills…and diplomacy…From a technical perspective each incident handler requires a basic understanding of the underlying technology and issues on which the individual will base their expertise."[4] The list is extensive. All of the skills are required to have a viable CIRT, but not in individual members. This skill set became the final section of the Charter and rounded up the basic presentation necessary for the Director's initial review.

Presentation and Acceptance

We developed an executive summary, potential measurements of success, a return on investment (ROI) discussion, and proposed follow-up actions in preparation for the Directors. The charter of the CIRT organization was presented at their quarterly meeting, with a detailed discussion by the policy team. A successful presentation was crucial for adoption so the team had discussions with a couple of Directors prior to the session. They would assist the team in bringing this proposal to the table with the best possibility of success. Management support was overwhelming once the presentation was complete there was very little discussion. The policy team was praised for its effort and encouraged to move the process of establishing a formal CIRT forward, full speed. This boosted the policy teams dedication to the effort and we redoubled our commitment. Management formally adopted the charter with minimal modification and has begun promoting it as an example charter for other agency-wide teams to utilize.

Next Steps

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Now the hard part begins. We have formally distributed an official letter requesting applications from interested individuals. Applications must go through supervisors and the Director for consideration. A resume documenting all experience and education must be included for applicants. In the meantime, the policy team has moved on to the next level of business, documenting policy and procedures for the CIRT to implement. We need to develop 1) a "Code of Conduct", 2) information categorization scheme, 3) an information disclosure policy, 4) a media policy, and 5) a CIRT security policy[4]. These will become the working documents to be used by CIRT in their response procedures. There are more ways to develop team procedures then there are ways to develop a charter. The policy team is planning a "sand-box" training session to test and refine process, which will take place as soon after team membership selections are made as feasible.

Summary

The agency has become more secure electronically, through our continuous education of management and employees, during the process of producing the charter. The organization originated and evolved with a "can do" attitude, with little knowledge of potential security issues and is using the same attitude to improve its security posture. We are significantly less compromised and are able to react with consensus and a justified policy when incidents occur. This was tested recently with the outbreak of the SoBig.C and SoBig.E virus threats. With SoBig.C the MRT was the initial resource to identify the actual occurrence rate and alert a larger audience of agency experts. Through this avenue an impromptu CIRT was organized. We were able to invest resources in a more organized and coordinated fashion, allocating responsibilities and reconvening periodically to share information and document gathered information, in the malware response repository. A decision was made, after much discussion, to use the tool available from Symantec to clean infected PCs. The response was communicated directly to the support center as well as documented in the repository. "If the user receives a message of an infection, immediately remove the box from the network and run a full virus scan. If an infection occurred the local computer support will be contacted to run the cleanup tool prior to the box being reconnected." During the SoBig. E incident the same basic response procedure was used. The MRT alerted and convened a temporary CIRT, which identified the risks. The team developed a consensus response and it was posted. The agency was better able to react to these occurrences, relaying the organizational response quicker and more efficiently than with SoBig.C. Considering last year's situation to this year's success verifies the benefits gained by training and coordination. An official CIRT would improve the situation even further.

The threat becomes clearer in all discussions with users and management, and the distribution of a CIRT charter has increased organizational awareness of the need for protection. The MRT has established the ground work for CIRT and the

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

users ability to communicate with a person and receive a coordinated, pre-established, uniform response to a security threat has significantly improved our credibility, the user communities understanding, and their acceptance of drastic measures when infections actually occur. In the case of SoBig.E, if the infection occurred a re-image of the PC was required. The MRT has been pleasantly surprised at the understanding of the user when this remedy is imposed. There is less debate with the user, and the local computer staff is more supportive of the decision. All participants know the process and understand it to be in the best interests of the agency. This has clearly been a learning experience for everyone involved.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

References

[1] Department Manual xxxx-xxx, Computer Incident Response Procedures Manual, October, 2001.

[2] John P. Wack, Establishing a Computer Security Incident Response Capability, NIST Special Publication 800-3, November, 1991. Accessed online via http://csrc.nist.gov/publications/nistpubs/800-3/800-3.ps, (7/6/03).

[3] Kenneth R. Van Wyk, Richard Forno, Incident Response, O'Reilly & Associates, Inc., 2001.

[4] Moira J. West-Brown, et al., Handbook for Computer Security Incident Response Teams, April 2003, Accessed online via http://www.cert.org/archive/pdf/csirt-handbook.pdf, (7/6/03).

[5] Carnegie Mellon Software Engineering Institute/CERT Coordination Center, Creating a Computer Security Incident Response Team, 2002. Accessed online via http://www.cert.org/csirts/Creating-A-CSIRT.html, (7/6/03).

[6] Simon Martinez, SecurityUnit.com, Federal Government Incident Response Team, April 23, 2002, Accessed online via http://secinf.net/misc/Federal Government_Incident_Response_Team_IRT.html, (7/6/03).

[7] Michael Miora, White Paper: Building an Incident Response Team, . November 14, 2002, Accessed online via http://www.contingenz.com/Building%20an%20IRT.pdf, (7/6/03).

[8] Bruce Schneier, Secrets and Lies, Digital Security in a Networked World, John Wiley & Sons, Inc., 2000.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

[9] Danny Smith, Australian Computer Emergency Response Team, The University of Queensland, January 1, 1995, Accessed online via http://www.auscert.org.au/render.html?it=2252&cid=1938, (7/6/03).

[10] Sanda International Corp., Sample Standard Practice for Implementation and Management of a Computer Incident Response Team, 1998, Accessed online via http://www.securityunit.com/pubs/cirt_std.doc, (7/6/03).

© SANS Institute 2003, Author retains full rights.

Bibliography

Carnegie Mellon Software Engineering Institute/CERT Coordination Center. Creating a Computer Security Incident Response Team: A Process for Getting Started. 2002. Accessed online via http://www.cert.org/csirts/Creating-A-CSIRT.html. (7/6/03).

Carnegie Mellon Software Engineering Institute/CERT Coordination Center. Computer Security Incident Response Team (CSIRT) Frequently Asked Questions (FAQ). 2002. Accessed online via http://www.cert.org/csirts/csirt_faq.html. (7/6/03).

Martinez, Simon. SecurityUnit.com. Federal Government Incident Response Team (IRT). April 23, 2002. Accessed online via http://secinf.net/misc/Federal Government_Incident_Response_Team_IRT.html. (7/6/03).

META Security Group. Developing a Security Incident Response Team (SIRT). 2002. Accessed online via http://www.metasecuritygroup.com/library/whitepapers/DevelopingASecurityIncidentResponseTeam.pdf. (7/6/03).

Miora, Michael. White Paper: Building an Incident Response Team (IRT). November 14, 2002. Accessed online via http://www.contingenz.com/Building%20an%20IRT.pdf. (7/6/03).

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Mitnick, Kevin D., William L. Simon. The Art of Deception, Controlling the Human Element of Security. Wiley Publishing, Inc. 2002.

Network Working Group. RFC 2350. Expectations for Computer Security Incident Response. June 1998. Accessed online via http://www.cis.ohio-state.edu/cgi-bin/rfc/rfc2350.html. (7/6/03).

Network Working Group. RFC 2196. Site Security Handbook. September 1997. Accessed online via http://www.cis.ohio-state.edu/cgi-bin/rfc/rfc2196.html. (7/6/03).

Sanda International Corp. Sample Standard Practice for Implementation and Management of a Computer Incident Response Team (CIRT). 1998. Accessed online via http://www.securityunit.com/pubs/cirt_std.doc. (7/6/03).

Schneier, Bruce. Secrets and Lies, Digital Security in a Networked World. John Wiley & Sons, Inc. 2000.

Smith, Danny. Australian Computer Emergency Response Team. The University of Queensland. January 1, 1995. Accessed online via http://www.auscert.org.au/render.html?it=2252&cid=1938. (7/6/03).

Van Wyk, Kenneth R., Richard Forno. Incident Response. O'Reilly & Associates, Inc. 2001.

Wack, John P. Establishing a Computer Security Incident Response Capability (CSIRC). NIST Special Publication 800-3. November, 1991. Accessed online via http://csrc.nist.gov/publications/nistpubs/800-3/800-3.ps (7/6/03).

West-Brown, Moira J., Don Stikvoort, Klaus-Peter Kossakowski, Georgia Kilcrece, Robin Ruefle, Mark Zajicek. Handbook for Computer Security Incident Response Teams (CSIRTs), April 2003. Accessed online via http://www.cert.org/archive/pdf/csirt-handbook.pdf. (7/6/03)./

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.