GCIH Practical Assignment

Name: Judith Westray
Version Number: GCIH Practical Assignment 1.5c
Title: Early Success for a New Incident Response Program

Section 1. Executive Summary

Company X (hereafter referred to as The Company) is a for-profit research subsidiary of one of the premier universities in the country. The Company has a very large network with over 50, 000 users and 1000 applications. The Company has a very distributed support environment and a large IT department. Only recently did the company add a security group. The security group was charged with building a security department from the ground up. One of the primary objectives of the security department was to develop an incident response program. Of course the hacker community didn't give the company the courtesy of striking after the incident response program was fully developed. Early in the development stages of the incident response program, hackers using the sadmind/IIS worm targeted The Company. The sadmind/IIS worm targets Sun Solaris boxes and then uses them to attack Microsoft IIS boxes.

Section 2. Description of 6 stages of incident handling

Corporate Background

Company X (hereafter referred to as The Company) is a for-profit research subsidiary of one of the premier universities in the country. The Company has a significant international presence and many of its employee's are not only world-renowned but also the worlds first, second or third top-ranking specialist in their area of expertise. The Company has a significant research arm and spends a considerable amount of income on Research and Development. The Company has significantly increased in size due to a series of mergers and acquisitions. The result is a corporation with over 50,000 users, 300+ customer areas, 700+ applications, 20 different hardware platforms, and 10 different OS platforms that are managed by the centralized IT department. In addition, it is estimated that there are 250+ applications and any number of hardware and operating system platforms located in departments and divisions that are not managed or known to the centralized IT department.

Security Posture

The Company has a centralized information technology organization (CITO) comprised of the usual departments (system (platform) support, database support, application development teams, PC support, etc.). While the CITO manages most of the information technology projects for The Company, various subsidiaries and departments have their own information technology staff that provides system support for oftentimes mission critical systems. As a result of its rapid growth and this distributed technology support structure, The Company does not have a complete understanding of the information systems. This condition makes it increasingly difficult to respond to security threats, develop procedures, etc. The Company recently added an Information Security Group to its centralized IT department. The Information Security Group was charged with developing a security program for the entire organization including:

- Performing a risk analysis
- Securing the perimeter
- Developing a comprehensive list of users, systems, and applications
- Implementing intrusion detection and policy compliance tools
- Drafting policies and standards
- Developing minimum security baselines for the CITO-supported
- Developing an incident response program

The development of the incident response program was one of primary goals of the new security group.

Preparation

Preparation involves establishing policies, procedures, and agreements in advance, to minimize the chance of making catastrophic mistakes[1]

Initially, The Company contracted a vendor to develop an Incident Response program for the entire organization. After spending a considerable amount of time responding to interviews/questionnaires and participating in design sessions, the final product turned out to be a generic boilerplate that is apparently provided to all of this vendors customers. This generic template clearly did not address the unique requirements of The Company. As a result the vendor was dismissed and The Company began development of an Incident Response program using the SANS Institute Step-by-Step guide and the Handbook for Computer Security Incident Response Teams as a guide.

An Incident Response Planning Team was assembled from the centralized IT organization and a Security Administrator from the Information Security Group. Technically, the purpose of this group was to develop a project plan, procedures and policies for computer security incident response. Politically, this group was formed to obtain buy-in and to develop a sense of ownership of the process from the other CITO support departments. Additionally, it was necessary to temper the unrealistic expectations that the Information Security Group, not allowed on machines, will come in during an event and assume admin privileges and heroically fix the problem.

While each of the Incident Response Planning Team members had a minimum of 15 years of information technology experience, none of them were experienced in security as a discipline and none had any experience or knowledge of the incident response process. The team used a memo on Computer Security Incident handling by The Department of Commerce to define or provide a general overview of the 6 steps of Incident Handling and the SANS Step-by-Step guide to identify the actual tasks associated with each step. Instead of developing a chronological task list, the approach the Incident Response Planning Team used to develop the project plan is unique in that the planning team took each step (Preparation, Identification, Containment, Eradication, Recovery, Lessons Learned) and identified the processes, tools, and documentation necessary to successfully perform the tasks associated with that phase. For example, the task list for the Containment phase includes the following items:

- Determine how to back up/save evidence on each platform for forensics.
- Identify non-networked backup hardware and software for each platform.
- Develop and document procedures for making backups for each platform.

The tasks for the Eradication phase includes items to:

- Identify and select tools to perform system vulnerability analysis.
- Develop procedures on how to locate the most recent clean backup after an incident.

As the Incident Response Planning Team gained a better understanding of the incident response process, it became increasingly obvious that a mature incident handling capability was not going to develop immediately. The scope of the Incident Response Planning Team changed to building an incident response framework and providing more detail over time. After a list of all the tasks had been completed, the IR Planning Team prioritized the items based on importance and practicality. The project plan was developed and distributed to the Directors of the groups with responsibility for project tasks.

In addition to developing a list of *what* needed to be done to prepare for an incident, it was also important for members of The Company to understand *who* did what. To that end, the IR Planning Team worked on customizing a document originally provided by the vendor explaining the roles of each of the departments/individuals during an incident. See Chart A for organization chart of incident response team. Following are examples:

System Administration Support

Definition:

Individuals responsible for the design, implementation, administration, and maintenance of operating systems, applications, system hardware, etc. Includes UNIX, Microsoft platforms & applications, VMS, NetWare, MPE, mainframe, desktop devices, server support, etc.

Function:

Based on CIRT policy, provide incident response planning and technical support to secure and recover The Company systems and networks.

Key Responsibilities:

- Assist in development and implementation of The Company CIRT policies, standards and procedures for platform/application support to the CIRT.

- Understand CIRT principles and The Company CIRT policies, standards, and procedures.
- Provide technical expertise necessary for intrusion detection, assessment, and response activities.
- Assist in the identification, selection and configuration of CIRT tools (backup devices, etc.).
- Monitor host systems and security tools as needed to support the CIRT areas of responsibility.
- Provide CIRT technical guidance to Health System entities.
- Provide system information (e.g. logs, configuration files) as required.
- Prepare periodic input to CIRT Status Reports and The Company CIRT Advisories.
- Participate in post-incident activities (lessons learned).

Legal Representative

Function:

Provide legal support and guidance to the CIRT on network monitoring, protection of evidence, and forensic investigations. Serve as direct interface with Law Enforcement agencies.

Key Responsibilities:

- Assist in development and implementation of CIRT standards and procedures requiring Legal assistance and guidance
- Work with The Company Data Protection Officer to determine legal approaches and actions
- Advise the Data Protection Officer and executive management on legal strategy relating to security incidents
- Work with law enforcement agencies to facilitate The Company legal responses.

Public Relations (Internal Communications)

Function:

Ensure any security incident-related internal releases or discussions follow established guidelines. Provide guidance for The Company staff (including all levels of management) and contractors on responsibilities and restrictions relating to internal communication of incident-related matters.

Key Responsibilities:

- Assist in development and implementation of CIRT standards and procedures requiring Public Relations support to the CIRT.
- Provide guidelines for internal communications related to Incident Response
- Disseminate CIRT information within Public Relations
- Be responsible for communications between the Public Relation

and The Company CIRT Team

Public Relations (External Communications)
Function:
Ensure any security incident-related external releases or discussions have been coordinated with The Company management. Provides guidance for The Company staff (including all levels of management) and contractors on responsibilities and restrictions relating to media contact and other forms of external communication.

Key Responsibilities:

- Assist in development and implementation of CIRT standards and procedures requiring News Bureau support to the CIRT.
- Provide guidelines for external communications related to Incident Response
- Act a primary interface for interaction with media
- Disseminate CIRT information within News Bureau organizations
- Be responsible for communications between the News Bureau departments and The Company CIRT Team

Human Resources
Function:
Support employee computer security awareness via signed computer use agreements and ensuring The Company employee policies relating to security are distributed to all employees.

Key Responsibilities:

- Supports CIRT internal investigations resulting in potential The Company disciplinary actions
- Manage The Company personnel issues related to security incidents
- Act as focal point for resolution and/or corrective action with The Company management.
- Disseminates CIRT information to Human Resources Department
- Be responsible for communications between the Human Resources department and The Company CIRT Team

Help Desk Staff
Function:
Based on CIRT policy, provide first-level triage and client support.

Key Responsibilities:

- Assist in the development and implementation of CIRT standards and procedures
- Provide call escalation for reported incidents
- Be responsible for communication to users and affected parties

based on PR Communication Guidelines for Incident Response

- Respond to user inquiries based on PR Communication Guidelines for Incident Response
- Provide reporting and analysis of computer incident activity
- Participate in post-incident activities
- Prepare periodic input to CIRT Status Reports

Meetings were held with members from each department to introduce the new Information Security Group, explain the incident response process (again using the memo on Computer Security Incident handling by The Department of Commerce) and to explain their role in the Incident Response process using the roles and responsibilities described above. The Information Security Administrator then worked with the various departments to develop basic procedures and polices for Incident Response. Detailed sessions were held with the Help Desk Staff to train the analysts on identifying security events, understanding the sensitivity of reported incidents, and communicating with users based on guidelines established by the PR department.

In addition, the following roles and responsibilities were identified for the Information Security Group when responding to incidents:

On-call Security Administrator

- Be available as a focal point during off-hours in the event of a security emergency
- Collect initial incident information
- Notify Incident Handler and Incident Investigator of issues as necessary
- Remain informed of response activity status to provide updates as required
- Monitor Help Desk security tickets.
- Respond to e-mails sent to the Information Security Group mailbox (account administration, virus, general inquiries, etc.)

Incident Investigator

- Own the problem from a technical aspect
- Collect and analyze detailed incident information (logs, trophies, etc.)
- Liaison with target system administrator and technical team.
- Identify post-incident project tasks

Incident Handler

- Prioritize incidents
- Identify and assemble required technical resources
- Manage response activities and escalate issues as necessary
- Verify response activities are in accordance with established procedures
- Manage communication to all involved parties (including response activities status and update and incident summary report)

The Incident Response Planning Team used the preparation phase not only to plan for the occurrence of an incident, but also as a means of education for themselves and other members of the organization about the incident response process. The Incident Response Planning Team had just completed some of the basic components of the Incident Response program before the incident covered in the rest of this document occurred.

Identification

Identification involves determining whether or not an incident has occurred, and if one has occurred, determining the nature of the incident.[2]

Because the incident involved actual modification of web sites, it was very easy to identify that an incident had occurred. The method of discovery in each case is outlined below:

1. At approximately 9:00 AM 5/7/2001, the CEO of Business Unit 1 reported the Business Unit 1 server web page defacement to a staff member. The staff member notified the CITO Help Desk, which followed the Incident Response triage procedures and immediately notified the Information Security Group.

2. At approximately 10:00 AM, 5/7/2001, a user of the Business Unit 2 server reported the page defacement to a Business Unit 2 server administrator. The server administrator's manager notified the Information Security Group at 11:30 on May 7, 2001

3. 5/9/01 various business units reported compromised servers.

4. At approximately 9:12 PM on 5/10/01, the Internic contact for the domain, received an e-mail from attrition.org that a Company website had been hacked and possibly defaced. The Internic contact verified the site defacement.

Coincidently during this series of incidents, the On-Call Security Administrator was also the individual who always functions as the Incident Handler. As a result, when the first incident was reported on 5/7/01, the Incident Handler was the first to be notified. The Incident Handler assumed responsibility and assigned a resource to investigate and make the initial assessment. Due to resource constraints the Incident Handler also acted as the Incident Investigator on the second reported web defacement. As additional reports were made the whole series of incidents remained the responsibility of the primary incident handler. Mainly this was a result of staffing and limited experienced resources however the side benefit of this was that it enabled the response team organization to do a better job of getting the "bigger picture". According to the Handbook for Computer Security Incident Response Teams, separate incidents should be compared with one another to get a better understanding of the "bigger picture". Refining the bigger picture is especially useful in identifying lessons learned and can help to improve response to future incidents. [3]

The incident investigators traveled to the targeted servers and obtained the IIS logs. The modified web pages and review of the IIS logs for the most part matched CERT Advisory CA-2001-11. Based on this information, the Incident Investigators determined that The Company web servers were compromised as a result of vulnerabilities exploited by the sadmind/IIS worm. CERT Advisory CA-2001-11 gives the following description of the sadmind/IIS worm:

> The sadmind/IIS worm exploits a vulnerability in Solaris systems and subsequently installs software to attack Microsoft IIS web servers. In addition, it includes a component to propagate itself automatically to other vulnerable Solaris systems. It will add "+ +" to the .rhosts file in the root user's home directory. Finally, it will modify the index.html on the host Solaris system after compromising 2,000 IIS systems.
> To compromise the Solaris systems, the worm takes advantage of two-year-old buffer overflow vulnerability in the Solstice AdminSuite sadmind program. After successfully compromising the Solaris systems, it uses a seven-month-old vulnerability to compromise the IIS systems.[4]

Sadmind (Sun Solstice AdminSuite) is a program used to perform remote system administration. Sadmind is installed by default on certain version of the Solaris operating system.[5]

Default html pages were replaced on a mail server and web server. The default page on both servers was replaced with an offensive alternative message (See CERT Advisory http://www.cert.org/advisories/CA-2001-11.html). No other activity was detected on the targeted servers

Containment

During this phase the goal is to limit the scope and magnitude of an incident in order to keep the incident from getting worse.[6]

In following with The Company's incident objective of containment and clean, the following actions were taken:

- Effected servers were taken off of the network.
- The Internet firewall ruleset was modified to prevent Any access to the targeted servers from Any IP addresses.

For each reported event, the Incident Investigator traveled to the site of the server and worked with the server's system administrator to obtain the logs. When available the logs were always obtained. In some cases, logging is not enabled. The logs were then stored and reviewed from the Investigators machine. At the time of this incident detailed procedures for obtaining and maintaining log files for use as possible evidence in court did not exist.

To prevent additional damage, the following actions were taken:

- Incident Handler directly contacted known non-CITO Unix administrators with instructions to follow the CERT recommended procedures for Solaris boxes.
- Incident Handler sent out notification to the known technical support community to begin to identify other machines that could be vulnerable
- Data Communications has provided a preliminary list of Unix servers on The Company network.
- All NT Administrator passwords changed.
- Reviewed firewall rule set to identify exposures presented by rules granted for targeted machines
- Had 8 instances removed from the Internet firewall rule sets:
  - 1 server from HTTP rule
  - 4 servers from the FTP rule
  - 3 servers from SMTP rule
- Notified Public Relations

Eradication

This phase ensures that the problem is eliminated and vulnerabilities that allow re-entry to the system are eliminated.[7]

Each server was reviewed to determine the best way to eliminate the problem (rebuild from vendor media, restore from backup, some combination). Each server was also looked at in terms of what minimum security baselines could be applied. The intention was that by eliminating the vulnerability to be exploited (applying patches, rebuilding machines with minimum security baselines), re-infection could be prevented.

Unix Servers

The Unix Support Team developed and implemented a plan for applying the CERT recommended patches. All CITO-managed Solaris servers were reviewed for sadmind status, patch level, and indication of inappropriate syslog entries and root .rhost file changes. Where necessary the following steps were taken:

- Sun recommended patch was applied using the following chart as a guide[8]:

OS Version	Patch ID
SunOS 5.7	108662-01
SunOS 5.7_x86	108663-01
SunOS 5.6	108660-01

SunOS 5.6_x86	108661-01
SunOS 5.5.1	108658-01
SunOS 5.5.1_x86	108659-01
SunOS 5.5	108656-01
SunOS 5.5_x86	108657-01

- The sadmind daemon was disabled by commenting out the appropriate line in the inetd.conf file

IIS Servers

The Web Services Team developed and implemented a plan for applying the CERT recommended patches. All CITO-managed IIS web servers were reviewed. The following steps were taken on machines that had not been compromised.

- Full backup was obtained
- The latest service pack was applied where necessary.
- The patch referenced in Microsoft Security Bulletin MS00-078 was applied where necessary

In addition a vulnerability scan was performed on the compromised servers using Symantec's NetRecon as well as an NT/IIS security-checking tool from the Center for Internet Security.

Given the available skill set, amount of resources available and the objective to contain and clean, a significant amount of time was not invested in determining how the intruder gained access.

Recovery

This phase ensures that the system is returned to a fully operational status.[9]

The NT servers that were compromised were rebuilt and hardened according to established minimum-security baselines developed by the Information Security Group. The compromised NT/IIS servers that were not managed by the centralized support group were moved under the auspices of the CITO. The rebuild process for these servers required each system to be built using original vendor installation media. The required Microsoft patches and hot fixes were applied.

The Information Security Group used this opportunity to configure the rebuilt machines to conform to all The Company's policies, standards and best practices. In addition, host-based intrusion detection was installed on each rebuilt web server.

The system owners and system administrators worked with the Incident Response Team to test and certify each system after rebuild. For the compromised server, a "super user" (user having significant knowledge and experience with an application) was identified for each application on the server. The super users tested each application to verify functionality. When all applications had been tested, the servers were put back on-line and the firewall ruleset was modified to allow external connectivity.

The Information Security Group initiated a project to follow-up with the other business units regarding their efforts in patching Solaris boxes and IIS servers.

Lessons Learned

This phase is important in identifying lessons learned that will prevent future incidents.[10]

Once the compromised servers were back on-line, a lesson learned session was held and attended by all of the major players involved in the incident. Initially getting the attendees to participate in the meeting was difficult. People were reluctant to call attention to things they didn't do correctly. The Incident Handler encouraged discussion by first listing a couple of things that went well and then pointing out things that the Handler wished he had done better or differently and then asking each member of the group if there was anything that the handler could have done to make their job easer during the response procedures. By pointing out his own failings and offering himself as a target, the Handler made people feel more comfortable in identify areas of improvement for themselves. The major points from the lessons learned session were documented and some of them are included in the chart below.

Lessons – Learned

Several key lessons were learned from these security incidents and are summarized in the points below.

	Successful	***Opportunities for Improvement***
Communication	• A central communication point was conducive to all essential players being informed and working together effectively.	• Procedures for reporting a security incident need to be better publicized to the user community. • Staff does not understand the importance of sharing security incident information on a need-to-know basis. The confidentiality surrounding the incident was not contained to essential players. • Essential players vary by incident. Initially a wider group of incident response participants needs to be involved for awareness and communication. • The use of a centralized timekeeping tool should be investigated for tracking time spent for incident response activities across all parties involved to provide a consolidated picture to management.
Response Activities	• Documented incident response procedures were followed by the Response Team.	• The escalation procedures and decision tree needs to be improved for a quicker response. • Urgency of incident-related response activities needs to be clearly defined. • IR Planning team should continue to develop processes and procedures.

Technical Procedures	• Unix Support is doing a good job of staying current with Sun recommended patches.	• The centralized IT department needs a better process for consistently monitoring, identifying and applying service packs, patches, and hot fixes. • System administrators need to be more familiar with their logs. • Logging should be enabled on all servers. MSB should be created that outlines minimum audit policy for each platform and class of system.

Section 3. Assessment and Containment process – Unix

While the CITO maintains comprehensive documentation on the servers it manages, systems that are managed by other business units or divisions are not part of any master list. As a result there was no quick way of locating all of the Sun Solaris boxes on The Company network that were vulnerable to the sadmind/IIS worm. The incident response team had to come up with some way of identifying the Sun Solaris servers on the network but not supported by the centralized IT department. The solution was to identify the Sun boxes by their Ethernet address using the OUI for Sun Microsystems.[11] To develop a list of sun boxes, we ran a query on MAC addresses. Using the UserTracking application in Cisco Works for Switched Internetworks (CWSI), we ran a query to look for the occurrence of MAC Address prefix "08:00:20" [12]

Once we had a list of machines, the contact person for each machine was identified and notified to follow the guidelines recommended in the Sun Microsystems bulletin for the Sadmind vulnerability[13].

For sun boxes managed by the centralized IT department, the following steps were taken.

1. Each machine was reviewed to see if the Solstice AdminSuite daemon was installed and/or enabled.[14]
2. The Solstice AdminSuite daemon was disabled on any machine in which it was found active by commenting out the appropriate line in the inetd.conf file.
3. The syslog file of any machine on which the sadmind daemon was running was reviewed.
4. The root user's .rhost file was reviewed.
5. The patch status of each machine was determined and checked against recommended patches
6. The recommended patch was applied if the machine had not received the recommended patch.

At this time, no jump kit had been created for use during incidents. It had been listed as an action item in the Incident Response Project Plan.

Section 4. Backup Process – NT

Because the incident response program is in the early stages of development, the servers were backed up so as not to impact availability after applying the IIS hot fixes and not necessarily to preserving evidence or perform forensic analysis. The NT servers involved in this incident are backed-up regularly to a Compaq DLT 40/80 GB internal tape drive using Veritas BackupExec.

A full backup was performed on each server using the Veritas copy method. The copy method as defined by Veritas backs up all selected files. Using this method, the archive bit is left intact so the files will appear to the system as not having been backed up. The copy method allows the back up of data without affecting the existing backup strategy[15].

Each backup was written to a new tape and held by the Web Services Manager. Initially, the application of the service pack or hot fixes caused the web site to lose some functionality. The server was restored from the backup. The Web Services and LAN teams re-applied the patches and hot fixes based on Compaq's recommendations and the site began working as normal. A plan for applying the CERT recommended patches to the IIS servers was developed based on the process used to update the initial server. This plan was also distributed to the business units and divisions with IIS servers.

Section 5. Chain of Custody procedures used

The chain of custody procedures used during this incident were not very strong. System logs were mailed to either the incident handler or incident investigator and stored on a shared drive. The most care was taken of the IIS server backups and that was mainly to ensure the availability of the backup tape in the event that the application of the hot fix or service pack introduced a problem to a production server.

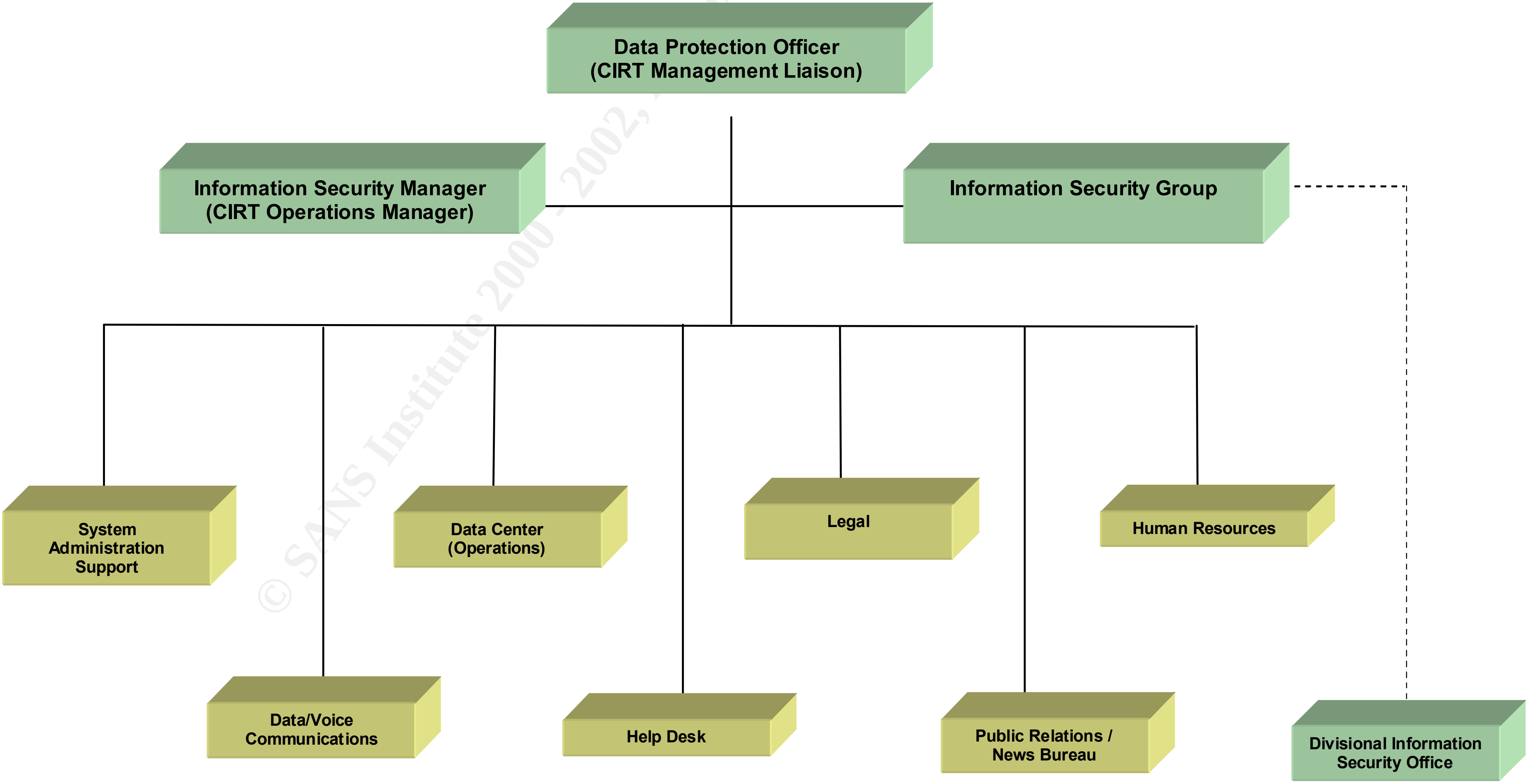
Given that the Incident response program is not very mature, more emphasis is being placed on the preparation, identification and containment phases. Since this incident has occurred, the Information Security Group has worked with the Physical Security Department to take advantage of the experience that they have with handling physical evidence. These existing procedures are being incorporated into the computer incident response chain of custody process.

Section 6. Citation of Sources

1. Baker, Roger W. http://www.doc.gov/cio/oipr/ITSECmemo7-9-99.htm
2. Carnegie Mellon University, CERT/CC. CERT® Advisory CA-1999-16 Buffer Overflow in Sun Solstice AdminSuite Daemon sadmind. March 2, 2000. URL: http://www.cert.org/advisories/CA-1999-16.html
3. Carnegie Mellon University, CERT/CC. CERT® Advisory CA-2001-11 sadmind/IIS Worm. May 10, 2001. URL: http://www.cert.org/advisories/CA-2001-11.html
4. Sun Microsystems. Security Bulletin #00191 – sadmind. December 29, 1999. URL: http://sunsolve.sun.com/pub-cgi/retrieve.pl?doctype=coll&doc=secbull/191&type=0&nav=sec.sba
5. The SANS Institute, Computer Security Incident Handling: Step-by-Step, version 1.5, May 1998.
6. VERITAS Software Corporation. VERITAS *Backup Exec for Windows NT® and Windows® 2000 Administrator's Manual,* 2000.
7. West-Brown, Moira J., Stikvoort, Don, Kossakowski, Klaus-Peter; Handbook for Computer Security Incident Response Teams (CSIRTs), Pittsburgh: Carnegie Mellon University, 1998

The Company CIRT ORGANIZATION

Chart A



Data Protection Officer
(CIRT Management Liaison)

Information Security Manager
(CIRT Operations Manager)

Information Security Group

System
Administration
Support

Data/Voice
Communications

Data Center
(Operations)

Help Desk

Legal

Public Relations /
News Bureau

Human Resources

Divisional Information
Security Office

End Notes

[1] Baker, Roger W. http://www.doc.gov/cio/oipr/ITSECmemo7-9-99.htm.

[2] Baker, Roger W. http://www.doc.gov/cio/oipr/ITSECmemo7-9-99.htm

[3] West-Brown, Moira J., Stikvoort, Don, Kossakowski, Klaus-Peter; page 70.

[4] CERT® Advisory CA-1999-16 Buffer Overflow in Sun Solstice AdminSuite Daemon sadmind.

[5] CERT® Advisory CA-2001-11 sadmind/IIS Worm.

[6] Baker, Roger W. http://www.doc.gov/cio/oipr/ITSECmemo7-9-99.htm

[7] Baker, Roger W. http://www.doc.gov/cio/oipr/ITSECmemo7-9-99.htm

[8] Sun Microsystems. Security Bulletin #00191 – sadmind.

[9] Baker, Roger W. http://www.doc.gov/cio/oipr/ITSECmemo7-9-99.htm

[10] Baker, Roger W. http://www.doc.gov/cio/oipr/ITSECmemo7-9-99.htm

[11] OUI (**O**rganizational **U**nique **I**dentifier) is defined as the part of the MAC address that identifies the vendor of the network adapter. The OUI is the first three bytes of the six-byte field and is administered by the IEEE.

[12]Cisco Works for Switched Internetworks (CWSI) is a suite of network management applications. CWSI applications enable you to configure, monitor, and manage a switched internetwork. CWSI includes the VlanDirector and UserTracking applications.

The UserTracking application enables you to access and modify information about end-user nodes in the CWSI and VMPS databases in a network. With UserTracking you query the CWSI database using up to two search criteria, including username, IP address, and MAC address.

[13] Sun Microsystems. Security Bulletin #00191 – sadmind.

[14] ScreenPrint

```
        Script started on Tue May 07 13:04:28 2001
        # showrev -p | grep 108660
```

```
Patch: 108660-01 Obsoletes:  Requires:  Incompatibles:  Packages:
SUNWadmfw

# exit


script done on Tue May 07 13:04:57 2001
```

[15] Veritas, page 68