Global Information Assurance Certification Paper

Advanced GCIH – Incident Handling and Hacker Exploits Practical Assignment (Version 2.0) Option 1 – Exploit in Action

A Study on incident Handling process

Win32-Nimda Worm

Submitted by: Sanjay Chakladar

Date: Jan 31, 2002

Table of Content

Part 1: Background of the Exploit

Interest & Motivation:
My practical is more of a study and research on this subject and particularly to explore different type of cyber-incidents that affects large organizations, their planning and recovery process to deal with such type of incidents and on-going surveillance process to safeguard their network and assets. Since I am not directly involved with the incident handling and response team most of the items I collected here are from different sources from the Internet and through interviewing my colleagues with in our firm. I selected the topic of Nimda, which affected our network in a big way by slowing down our network and in some case, shutting down the network – a complete denial of service. Interestingly initial Nimda virus/worm hit us on September 18, 2001 and while people were working on cleaning up all the servers and affected desktop, a variant of this worm (Nimda.e) hit many of our server again in first week of November 2001.

Background:
Nimda is a computer worm which first appeared on September 18, 2001, caused traffic slowdowns as it rippled across the Internet, spreading through four different methods, infecting computers containing Microsoft's Internet Information Server (IIS) Web servers and computer users who opened an e-mail attachment. Like a number of predecessor viruses, Nimda's payload appears to be the traffic slowdown itself - that is, it does not appear to destroy files or cause harm other than the considerable time that may be lost to the slowing or loss of traffic known as denial of service (DoS) and the restoring of infected systems. With its multi-pronged attack, Nimda appears to be the most troublesome virus of its type that has yet appeared. Its name (backwards for "admin") apparently refers to an "admin.DLL" file that, when run, continues to propagate the virus.

Name: Nimda
Nimda is “admin”, short for “system administrator”, spelled backwards. This worm is also known as “readme.exe” and W32/Nimda@MM, I-Worm Nimda (AVP), Nimda (F-Secure), W32.Nimda.A@mm (NAV), W32/Mnida@MM, W32/Nimda.eml, W32/Nimda.htm, W32/Nimda@MM, CV-5, Concept Virus, Code Rainbow, Nimda.A (Trend), Mimda and Win32.Nimda.A@mm (AVX).

Common Vulnerability and Exposures (CVE) number CA-2001-26

Exploit:
The worm exploits four known Microsoft vulnerabilities

- **Microsoft IIS/PWS Escaped Characters Decoding Command Execution Vulnerability** http://www.securityfocus.com/bid/2708
- **Microsoft IE MIME Header Attachment Execution Vulnerability** http://www.securityfocus.com/bid/2524
- **Microsoft IIS and PWS Extended Unicode Directory Traversal Vulnerability** http://www.securityfocus.com/bid/1806

- **Microsoft Office 2000 DLL Execution Vulnerability**
  http://www.securityfocus.com/bid/1699

- It probes each IP addresses within a randomly selected range of IP addresses, attempting to exploit weaknesses that, unless already patched, are known to exist in computers with Microsoft's Internet Information Server. A system with an exposed IIS Web server will read a Web page containing an embedded JavaScript that automatically executes, causing the same JavaScript code to propagate to all Web pages on that server.
- As people (those with Microsoft Internet Explorer browsers at the 5.01 or earlier level) visit sites at the infected Web server, they download pages with the JavaScript that automatically executes, causing the virus to be sent to other computers on the Internet in a somewhat random fashion.
- Nimda also can infect users within the Web server's own internal network that have been given a network share.
- Finally, once Nimda has an infected system do is to send an e-mail with a "readme.exe" attachment to the addresses in the local Windows address book. A user who opens or previews this attachment (which is a Web page with the JavaScript) propagates the virus further.

Alias:
Concept5, Code Rainbow, Minda

Variants :

Name	Type	Differences/Variant
W32/Nimda.b@MM	Internet Worm	This variant is packed with a PE packer and the filenames README.EXE and README.EML are replaced with PUTA!!.SCR and PUTA!!.EML respectively.
W32/Nimda.d@MM	Internet Worm	This variant uses different filenames. README.EXE is now SAMPLE.EXE MMC.EXE is now CSRSS.EXE ADMIN.DLL is now HTTPODBC.DLL
W32/Nimda.e@MM	Internet Worm	Functionally the same as the D variant; minor differences only. The new variant includes two dynamic link library, or DLL files, COOL.DLL and HTTPODBC.dlll. Other files different from the original include SAMPLE.EXE, SAMPLE.EML, and RICHED20.DLL
W32/Nimda.f@MM	Internet Worm	Functionally the same as the D variant; minor differences only.
W32/Nimda.g@MM	Internet Worm	Functionally the same as the D variant; minor differences only.

Protocols/Services:
HTTP, SMTP, TFTP, NetBIOS

Operating Systems:
Win 95, Win 98, Win ME, Windows NT and Wnidows/2000
Microsoft Web Servers IIS 3.0, 409, 5.0;
Microsoft Personal Web Server (PWS) 1.0, 3.0

Advisories & References:

National Infrastructure Protection Center Advisory 01-022, September 18th, 2001

Carnegie Mellon CERT Coordination Center Advisory CA-2001-26, September 18th, 2001.

http://www.cert.org/body/advisories/CA200126_FA200126.html

http://www.f-secure.com/v-descs/nimda.shtml

Part 2 – The Attack

Overview of the exploit[1]

Nimda worm propagate itself to new victims via four different ways:

1. The worm scans the Internet looking for web servers and attempts to exploit a number of Microsoft web server vulnerabilities to gain control of a victim host. It attacks victim's network by exploitation of the "IIS/PWS Extended Unicode Directory Traversal Vulnerability", the "IIS/PWS Escaped Character Decoding Command Execution Vulnerability", and utilization of backdoors left behind by previous Code Red II and Sadmind infections. Once in control of a victim IIS/PWS server, the worm uses TFTP to transfer its code from the attacking machine to the victim. The file transferred via TFTP is named "Admin.dll". Microsoft IIS 3.0, 4.0, and 5.0 are all affected, as well as are Personal Web Server (PWS) 1.0 and 3.0.
2. The worm uses email addresses from the Windows address book, user's inboxes/outboxes, and local HTML/HTM files and sends itself to all addresses as an attachment named "readme.exe". Any email software (x86 based) that uses a vulnerable version of Internet Explorer to display HTML messages will automatically execute the malicious attachment if the message is merely opened or previewed. This happens because the worm MIME encodes the attachment to take advantage of a known vulnerability called "Automatic Execution of Embedded MIME Types". Microsoft's Outlook and Outlook Express are the most typical victims. Then every ten days the worm regenerates its list of email addresses and sends itself to all.
3. If the worm successfully infects a web server, it uses the HTTP service to propagate itself to clients that browses the web server's pages. Upon infecting a victim server, the worm creates a MIME-encoded copy of itself named "README.EML" and traverses the directory tree searching for web-related files such as those with .HTML, .HTM, or .ASP extensions. Each time the worm finds a web content file; it appends a piece of JavaScript code to the file. The JavaScript code forces a download of README.EML to any client that views the file via a browser. Some versions of Internet Explorer will automatically execute the README.EML file and allow the worm to infect the client. The IE vulnerability issue here is the same as in the email propagation mechanism; that is, IE 5.5 SP1 or earlier is vulnerable to the "Automatic Execution of Embedded MIME Types" problem. Allowing JavaScript in the browser enables the worm to take advantage of the IE vulnerability.
4. The worm is network aware and propagates via open file shares. It will copy itself to all directories, including those found on a network share, for which the user has write permission. The worm places copies of "Riched20.dll" in multiple places on every accessible hard drive where files containing .DOC and .EML reside. Whenever the user opens a program that uses "Riched20.dll", it executes the worm. Files that use the riched20.dll are: Word, WordPad, and other editing programs. The worm will search the shared drives for executables, and attach itself to each executable it finds. Any other host that accesses the share and loads one of these files can become infected.

[1] www.incident.org - Paper on Nimda at:www.incidents.org/react/nimda.pdf

An Overview of the exploit Nimda.e

"W32.Nimda.E@mm is a new version of W32.Nimda.A@mm that contains bug fixes and other modifications, which are designed to prevent detection of this variant by anti-virus programs. The worm is similar in functionality to W32.Nimda.A@mm. Differences include the modification of file names used by the worm.

- The attachment received has been changed to: Sample.exe
- The dropped .dll file is now: Httpodbc.dll
- The worm now copies itself the \Windows\System folder as Csrss.exe instead of mmc.exe."

As far as propagation mechanisms, the new variant still emails itself as an attachment (now called Sample.exe), infects open network shares, attempts to download itself via web browsers, and attempts to inject itself into vulnerable IIS servers.

The new variant includes two dynamic link library, or DLL files, COOL.DLL and HTTPODBC.dlll. Other files different from the original include SAMPLE.EXE, SAMPLE.EML, and RICHED20.DLL. The web logs generated by a Nimda.E attack are somewhat different from the familiar Nimda pattern

Protocol description.

TCP/IP- Transmission Control Protocol/Internet Protocol, is a suite of communication protocols used to connect hosts on the Internet. This is the primary protocol used on our network and for connecting to the Internet.

Net BIOS-TCP port 137-139, 445- (Network Basic Input Output System) is an application-programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the Net BIOS. Net BIOS is based on the Server Message Block (SMB), SMB over NetBIOS uses port udp/137 for NetBIOS name services, udp/138 for NetBIOS datagram services or tcp/139 for NetBIOS session service. Window 2000 includes support for running SMB without NetBIOS over tcp/445, referred as Direct Host. Since we are running Windows client and Windows servers, Net BIOS is used to share files, directories and devices. These ports are used in the transmission of the worm to other computers that the infected computer shares files with.

HTTP- TCP port 80- The Hypertext Transfer Protocol (HTTP) is the protocol for exchanging files (text, graphic images, sound, video, and other multimedia files) on the **World Wide Web**. HTTP, the World Wide Web application protocol that runs on top of the Internet's **TCP/IP** suite of protocols. Relative to the **TCP/IP** suite of protocols (which are the basis for information exchange on the Internet), HTTP is an application protocol for web. Essential concepts that are part of HTTP include (as its name implies) the idea that files can contain references to other files whose selection will elicit additional transfer requests. For example, when you enter a URL in your browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested Web page. HTTP is called a stateless protocol because each command is executed independently- without any knowledge of the commands that came before it. The worm uses this port to target web servers to exploit known IIS vulnerabilities.

SMTP- TCP port 25- (Simple Mail Transfer Protocol) is a protocol for sending e-mail messages between servers. Most e-mail systems that send mail over the Internet use SMTP to send messages from one server to another. The messages can then be retrieved with an e-mail client. In addition, SMTP is generally used to send messages from a mail client to a mail server and is used by the worm in this capacity.

TFTP- UDP port 69- (Trivial File Transfer Protocol) is a simple form of the File Transfer Protocol (FTP). TFTP uses the UDP and provides no security features. This port is used to transfer the worm from one system to another.

Microsoft Internet Information Server- Also known as IIS is Microsoft's Web Server that runs on Windows NT/2000 platforms.

Internet Explorer Browser – Microsoft's web browser. Internet Explorer enables you to view Web pages.

How the exploit works

Attacking the Microsoft IIS Web Servers:

In this method, the worm spreads by excessively scanning local networks and the Internet for Web Servers - specifically targeting systems running Microsoft's Internet Information Server software. The worm searches for systems vulnerable to one of two well-known security vulnerabilities (IIS/PWS Extended Unicode Directory Traversal Vulnerability and IIS/PWS Escaped Character Decoding Command Execution Vulnerability) to copy the file, "admin.dll" to that server. Nimda also searched for systems that have been compromised by the Code Red II worm- and uses the backdoor placed on those systems to copy itself ("admin.dll") to the server. Once it finds a web server that is vulnerable to the Unicode attack or the Code Red II backdoor (e.g. exploit the root.exe backdoor left by

Code Red II or possibly Sadmind infections), it uploads Admin.dll via tftp to the machine being infected.

Once a web server is infected, all .HTML, .HTM, and .ASP files are identified and a piece of JavaScript is appended to each file. Nimda then adds a multi-part MIME-encoded copy of the worm, named readme.eml in the directories where these files are found. This system is now a portal for web surfers to be infected.

It is important to note here that if a server was patched for IIS vulnerabilities but had been infected with the Code Red II worm in the past and the backdoor was not removed, the system was still vulnerable to the Nimda worm. This was the reason why Nimda.e hit our network again in November.

WEB BROWSER-BASED PROPAGATION
The web browser based infection can be spread through viewing an infected Web page. If JavaScript is enabled in a users browser, and attempt to access and view an infected web page will result in a copy of the worm (now named "readme.eml"), to be downloaded to the users computer. The worm will run automatically with systems that have Microsoft's Internet Explorer 5.5 SP1 or earlier that have not been patched. Patched systems will prompt the user's permission to download the file. Either way, just viewing the infected web page may infect the user.

E-mail Propagation

With this method, the Nimda worm arrives to a system as an embedded e-mail attachment. The body is usually empty while the subject field of the e-mail is usually long and repetitive. The email contains a file, README.EXE, as an attachment. The version of Internet Explorer on the users computer will determine if the file will be executed automatically (without the user's intervention or knowledge) or will require the user to click on the attachment in order for it to be executed. The writer of this worm took advantage of a known vulnerability in Internet Explorer 5.5 Service Pack 1 or earlier (excluding Internet Explorer 5.01 Service Pack 2) and has used this vulnerability to propagate the Nimda worm even further than would a worm that relies solely on user intervention to open an attachment in order for the execution of the file to take place. It is interesting to note that when the system has Outlook or Outlook Express programs installed, and is patched for the old MIME (multipurpose Internet mail extensions) vulnerability (MS00-020), the system will actually prompt the user for permission to open the file and thus increases the likelihood of the spread of this worm. This likelihood is increased because most users will pick the default prompt and thus open the e-mail attachment.
Once a system is infected, the Nimda worm retrieves e-mail addresses from the use of Messaging API's and MAPI's and gets addresses from .HTML and .HTM documents found at the registry location:

HKCU/Software/Microsoft/Windows/CurrentVersion/Explorer/Shell Folder, Cache

The Nimda worm then uses an SMTP engine in the virus code itself to send out unsolicited e-mail to all these findings with the infected attachment.

The e-mail propagation is set to a cycle of every ten to eleven days. The worm stores a counter in the following registry location:
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MapMail, Cache

Once the worm runs, it resets its counter to start the countdown again. This will continue until the worm is removed from the system.

Another means of transmission has been via an e-mail attachment that appeared to originate from the Security Focus Aris Analyst team and Trend Micro[2]. The attachments name FIX_NIMDA.EXE, is very similar to Trend Micro's free tool to remove the Nimda worm from a system, FIX_NIMDA.COM. Security Focus has since released a memo to its distribution list warning users that this is a hoax and the attachment should not be opened.

NetBIOS share propagation

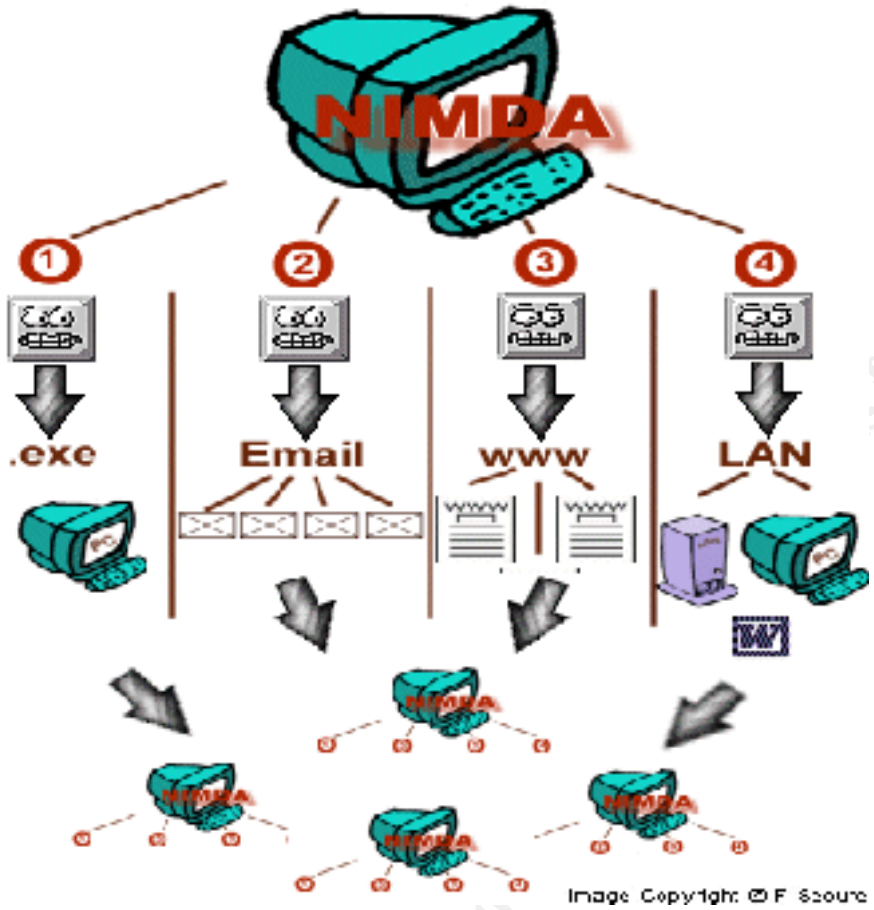
Spreading through network shares is another way to spread this worm. The worm places copies of "Riched20.dll" in multiple places on every accessible hard drive where files containing .DOC and .EML reside. Whenever the user opens a program that uses "Riched20.dll", it executes the worm. Files that use the riched20.dll are: Word, Wordpad, and other editing programs. The worm searches for file shares on file servers and workstations on the local network. The worm shares the C:\ drive with full access privileges and deletes all subkeys from:

SYSTEM\CurrentControlSet\Services\lanmanserver\Shares\Security

This is done to disable sharing security on the infected system.

The Worm propagation diagram:

[2] http://www.securityfocus.com/archive/75/217456



Signature of the Attack

The Nimda worm can be difficult to detect because the infections are different dependent upon the name of the file that started the infection process. Additionally, the Nimda worm attempts to hide itself on the infected system. The best way to test a system is to run an anti-virus scanner on the system to test for infected files.

Nimda changes registry entries that control viewing hidden files and extensions. It is therefore necessary to choose the View, Folder Options, View Tab in the Windows Explorer when looking in directories. Check these settings whenever you search a different directory. Nimda will continue to change the settings back to the hidden, so you must check the settings each time you begin a new directory search. If you change these settings and a few minutes later find out that the same directory has been changed back, it is a good indication that the worm is active in your system.

The worm has a copyright text string that is never displayed but reads, "Concept Virus (CV) V.5, Copyright ©2001 R.P. China".

IIS Web Servers

An infected Web Server will experience a dramatic increase in outbound traffic originating from the infected server. It will also experience an increase in dropped outbound traffic bound for port 80 at the firewall. The firewall may report or display unusual activity or cease functioning as a result of high traffic volume.

The server Intrusion Detection System (IDS) may show an increase in IDS alerts matching Unicode and CodeRed signatures. These alerts will have a consistent attacker IP address and inconsistent victim IP addresses.

Check for the admin.dll file in the web server's \scripts directory. This file should be found in the _vti_bin_vti_adm directory because this is the FrontPage extension for administering a website. It should not be found in the \scripts directory.

If the file is found, open the suspect admin.dll file in notepad, you will find the following strings:

(--====_ABC1234567890DEF_====), the string after src= in the <iframe> tag (3Dcid:EA4DMGBP9p), and the name of the attachment (name="readme.exe").

```
boundary="====_ABC1234567890DEF_===="
X-Priority: 3
X-MSMail-Priority: Normal
X-Unsent: 1

--====_ABC1234567890DEF_====
Content-Type: multipart/alternative;
        boundary="====_ABC0987654321DEF_===="

--====_ABC0987654321DEF_====
Content-Type: text/html;
        charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable


<HTML><HEAD></HEAD><BODY bgColor=3D#ffffff>
<iframe src=3Dcid:EA4DMGBP9p height=3D0 width=3D0>
</iframe></BODY></HTML>
--====_ABC0987654321DEF_====--

--====_ABC1234567890DEF_====
Content-Type: audio/x-wav;
        name="readme.exe"
Content-Transfer-Encoding: base64
Content-ID: <EA4DMGBP9p>
```

Run a search for the RICHED20.DLL and README.DLL in directories that contain .DOC or .EML files. Remember to turn off file hiding to ensure that you see them. Look in the web folders that contain .HTM, .HTML, or .ASP files for README.EML.

On Clients

Run a search for the README.EXE in the email attachments directory. Also, look for files in the temporary directory (\temp, \windows\temp, \winnt\temp) with the name MEP*.TMP and MEP*.TMP.EXE. Look for LOAD.EXE in the \windows or \winnt directories. Open the \windows\system.ini file with a text editor like notepad and look for the line: "shell=explorer.exe load.exe -dontrunold". If you find any of these files, your system is infected. You also may experience unexpected launches of Windows Media Player or RealPlayer on infected client machines.

Detecting Infected Packet Traffic

To detect infected packet traffic you must find unique strings. The following strings are detectible in the unpacked ADMIN.DLL and README.EXE executables, and in the infected e-mail message. Some easy to spot markers are the mime tags

(--====_ABC1234567890DEF_====), the string after src= in the <iframe> tag (3Dcid:EA4DMGBP9p), and the name of the attachment (name="readme.exe").

```
boundary="====_ABC1234567890DEF_===="
X-Priority: 3
X-MSMail-Priority: Normal
X-Unsent: 1

--====_ABC1234567890DEF_====
Content-Type: multipart/alternative;
        boundary="====_ABC0987654321DEF_===="

--====_ABC0987654321DEF_====
Content-Type: text/html;
        charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable


<HTML><HEAD></HEAD><BODY bgColor=3D#ffffff>
<iframe src=3Dcid:EA4DMGBP9p height=3D0 width=3D0>
</iframe></BODY></HTML>
--====_ABC0987654321DEF_====--

--====_ABC1234567890DEF_====
Content-Type: audio/x-wav;
```

name="readme.exe"
Content-Transfer-Encoding: base64
Content-ID: <EA4DMGBP9p>

Infected Web server attack packets contain some well-known ISS exploits. The following traffic is used to scan a web server for vulnerability. If a server gives a positive response for any of these attacks, the worm sends over attack code that attempts to download ADMIN.DLL using TFTP from the attacking site.

The scanning activity of the Nimda worm produces the following log entries for any web server listing on port 80/tcp:

GET /scripts/root.exe?/c+dir
GET /MSADC/root.exe?/c+dir
GET /c/winnt/system32/cmd.exe?/c+dir
GET /d/winnt/system32/cmd.exe?/c+dir
GET /scripts/..%5c../winnt/system32/cmd.exe?/c+dir
GET /_vti_bin/..%5c../..%5c../..%5c../winnt/system32/cmd.exe?/c+dir
GET /_mem_bin/..%5c../..%5c../..%5c../winnt/system32/cmd.exe?/c+dir
GET
/msadc/..%5c../..%5c../..%5c/..\xc1\x1c../..\xc1\x1c../..\xc1\x1c../winnt/system32/cmd.exe
?/c+dir
GET /scripts/..\xc1\x1c../winnt/system32/cmd.exe?/c+dir
GET /scripts/..\xc0/../winnt/system32/cmd.exe?/c+dir
GET /scripts/..\xc0\xaf../winnt/system32/cmd.exe?/c+dir
GET /scripts/..\xc1\x9c../winnt/system32/cmd.exe?/c+dir
GET /scripts/..%35c../winnt/system32/cmd.exe?/c+dir
GET /scripts/..%35c../winnt/system32/cmd.exe?/c+dir
GET /scripts/..%5c../winnt/system32/cmd.exe?/c+dir
GET /scripts/..%2f../winnt/system32/cmd.exe?/c+dir

Note: The first four entries in these sample logs denote attempts to connect to the backdoor left by Code Red II, while the remaining log entries are examples of exploit attempts for the Directory Traversal vulnerability.

How to protect against Nimda:

Users with web servers compromised by Nimda are advised to replace all modified files, and to carry out a full security audit. One of the exploits by which Nimda attacks servers relies on holes left behind by a previous Troj/CodeRed-II attack - and Nimda itself tries to open additional security holes, such as giving administrative powers to the "guest" user, which is supposed to be a highly restricted account.

Microsoft has issued a security patch, which reportedly secures IIS against the web server folder traversal vulnerability. It is available at http://www.microsoft.com/technet/security/bulletin/ms00-078.asp.
(This patch fixes a number of vulnerabilities in Microsoft's software, including the one exploited by this virus.)

For end Users

1. Prevent infection from email or infected Web sites by updating Internet Explorer as detailed as given in the Microsoft site in the section titled "Email" prevention. Patches and updated versions of IE have been available for some time to eliminate the vulnerability from Microsoft site. Customers who have installed any of the following updates would be at no risk of infection by email:
    - The patch provided in Microsoft Security Bulletin MS01-020.
    - The patch provided in Microsoft Security Bulletin MS01-027.
    - Internet Explorer 5.01 Service Pack 2.
    - Internet Explorer 5.5 Service Pack 2.
    - Internet Explorer 6. (If you are installing IE 6 as an upgrade on a Windows 95, 98, 98SE or ME system, be sure to select Full Install as the installation type).
2. Prevent infection via file shares by ensuring that you have no unprotected file shares, as discussed below:
    - To protect against infection via File Sharing, minimize the number of users who can access your file system. If you have file shares you do not need, remove them. For any remaining ones, ensure that you've given other users as few privileges as possible. Finally, if you're using Windows NT 4.0 or Windows 2000, make sure that you have a strong password for the Administrator account – if you leave it blank, you've essentially given the world the ability to add files to your system. The Microsoft Personal Security Advisor (available for Windows NT 4.0 and Windows 2000) can help ensure that your system is securely configured.

For System Administrators

1. Ensure that all workstations on your network are protected against infection from email or infected Web sites by installing any of the updates listed in the section below:

- The patch provided in Microsoft Security Bulletin MS01-020.
- The patch provided in Microsoft Security Bulletin MS01-027.
- Internet Explorer 5.01 Service Pack 2.
- Internet Explorer 5.5 Service Pack 2.
- Internet Explorer 6. (If you are installing IE 6 as an upgrade on a Windows 95, 98, 98SE or ME system, be sure to select Full Install as the installation type).

2. Protect Web servers by taking two steps:

   - Protect against the Code Red II worm, which leaves a "back door" that Nimda exploits, by installing any of the updates listed below in the section titled **Web Server Protection guidelines from Microsoft.** Servers that already have been infected can be cleaned using a tool Microsoft provides.
   - Block the "Web Server Folder Traversal" vulnerability by taking any of the steps listed below under **Web Server Protection guidelines from Microsoft**.
   - Prevent spread through file shares by ensuring that your workstations and servers have no unprotected file shares.

Web Server Protection guidelines from Microsoft:

A tool is available to remove the back door created by the Code Red II worm. However, the best course of action is to prevent the Code Red II worm altogether, by taking any of the following steps:

- Applying the patch provided in Microsoft Security Bulletin MS01-033
- Applying the patch provided in Microsoft Security Bulletin MS01-044
- Installing the Windows NT 4.0 Security Roll-up Package
- Running the IIS Lockdown Tool in its default mode

- Installing the URLScan tool with its default rule set.

Taking any of the following actions can block the "Web Server Folder Traversal" vulnerability:

- Applying the patch provided in Microsoft Security Bulletin MS00-057
- Applying the patch provided in Microsoft Security Bulletin MS00-078
- Applying the patch provided in Microsoft Security Bulletin MS00-086
- Applying the patch provided in Microsoft Security Bulletin MS01-026
- Applying the patch provided in Microsoft Security Bulletin MS01-044
- Installing Windows 2000 Service Pack 2
- Installing the Windows NT 4.0 Security Roll-up Package
- Running the IIS Lockdown Tool in its default mode
- Installing the URLScan tool with its default ruleset.

Microsoft has also issued a patch, which secures against the incorrect MIME header vulnerability, which can be downloaded from http://www.microsoft.com/technet/security/bulletin/MS01-027.asp.
(This patch fixes a number of vulnerabilities in Microsoft's software, including the one exploited by this virus.)

For more information on how to protect your systems against Nimda please follow this link: http://www.microsoft.com/technet/security/topics/Nimda.asp.

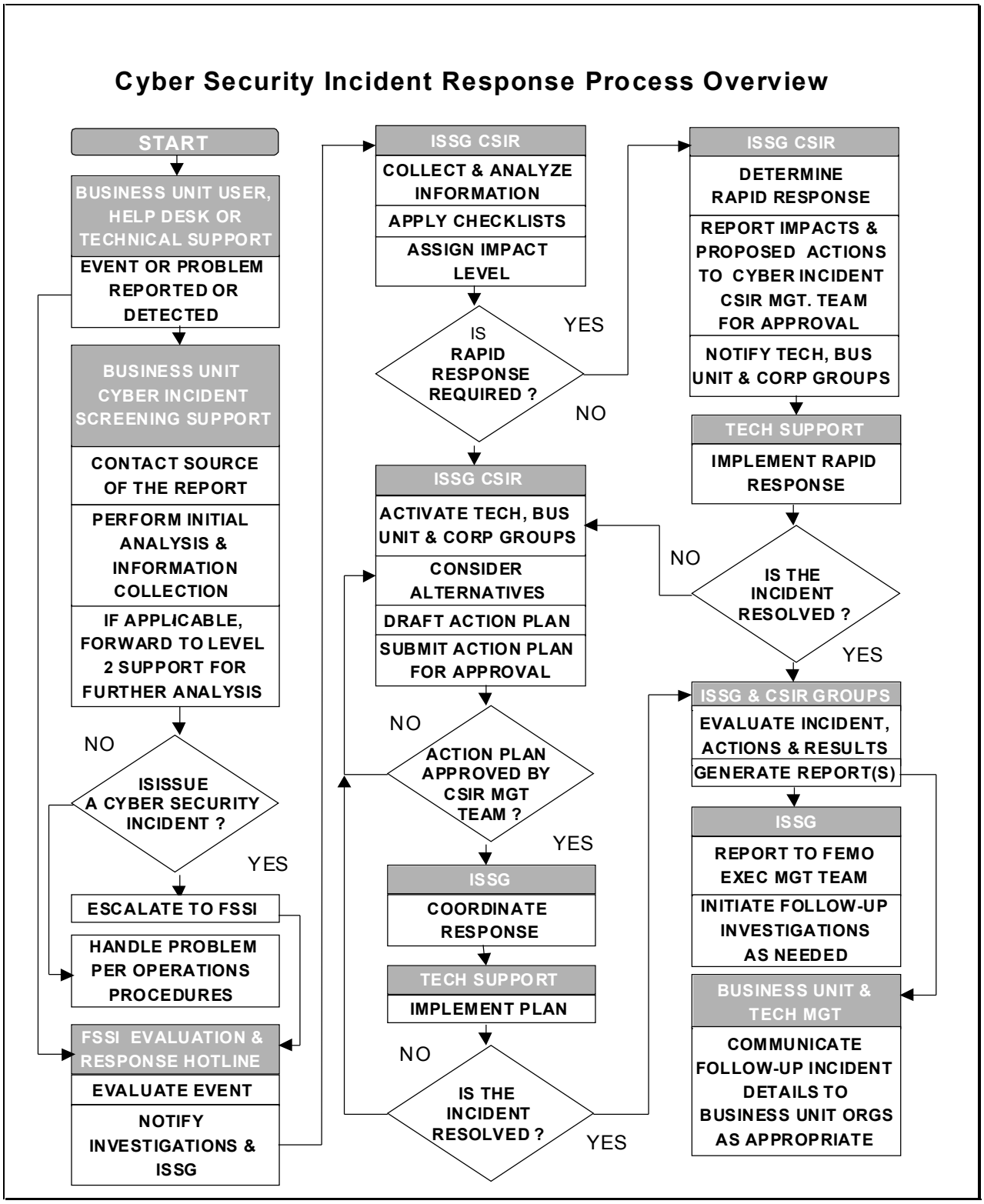
Microsoft makes available patches to secure against vulnerabilities in its products at: http://www.microsoft.com/technet/itsolutions/security/current.asp.

Part 3 – The Incident Handling Process

Preparation and Planning:

In our company ABC – henceforth referred as the company, has an Information Security team who is responsible for computer security and computer related emergency incident handling and response. The cyber incident and handling plan was prepared in late 1999 and was communicated to different business units. A Cyber Security Incident Response Business Unit Guidelines (see Attachment 1) was published and a team was designated to address any Cyber incidents. Based on these preparations, our team could put together a quick response plan to address this incident and prevented it from spreading across all over the company network and servers.

I described the flow chart of the Cyber incident Process flow in the next section:



Also the following information were circulated to every employee as part of the cyber incident awareness program:

How to Report a Security Incident or Risk

To report a potential information security incident or risk, please refer to the incident / risk specific reporting instructions below:

- **Virus Infections**: contact your business unit's help desk or the Customer Support Center using the CSC's "Report A Virus" web page http://XXX.XXX.XXX/Virus/report.htm or by calling directly at 1-800-XXX-XXXX.

- **Cyber Incidents**: Refer to your business unit's cyber incident response escalation plan or contact your Information Security Officer (ISO). If you are unable to contact your ISO and the matter requires immediate attention, please contact the company's Corporate Cyber Incident Response Team via Corporate Security's 24-hour Evaluation & Response Line at (XXX) XXX-XXXX. For more information on what a cyber incident is, indicators of a cyber incident and further response instructions refer to:

  Handling Suspected Cyber Incidents: A Guide For Systems Administrators (Annexure 1)

- **Other Information Security Incidents/Risks**: If you become aware of any other type of information security incident or risk, you should notify your Information Security Officer (ISO) or Business Information Security Director (BISD) immediately. See list of Information Security Officers for contact information. Alternatively, you can notify Information Security Group directly.

Additionally a comprehensive Intranet Site was developed for educational and awareness purposes for all employees regarding the Cyber incident and risk. The web site addressed the following information for all employees (see Annexure 2):

- Cyber security awareness by developing FAQ
- Cyber incident handling process
- Important contact information
- Important virus alerts and patch information

Identification, Containment, Eradication and Recovery Process:

On September 18, our network experienced some abnormal traffic patterns and also received the advisories from the external sources as well as our virus protection vendors. As an immediate step a Virus response team was setup that started to lookup different NT and Win 2000 servers. Immediately we identified that about 150 (out of 2000) different servers were infected by Nimda.a signature. Our firewall rule was set up to not accepts any executable attachment however company still allowed employee to access via http port 80 to public mail servers such as yahoo mail or hotmail etc. It seems we got hit via this route and were lucky that it was identified in the early stages and immediately access to public mail access was closed. Subsequently the following steps were taken which are described in detail as:

- Creation of multiple Virus SWAT team
- Isolation of the mail servers from the network
- Isolation of the affected network segments
- Swat team dispatched to all major Networks for detail scan and eradication
- Door poster and voice messages were delivered to each Business units and their employess.

- **W32.Nimda Vulnerability Scanning** - Corporate Security started working jointly with business units to identify and patch vulnerabilities that Nimda exploits. Information Security Officers will be expected to ensure that patching takes place within their business units and to report patching results to Corporate Security.
- **Trend Message Storage Area Scanning** – The company's Messaging & Groupware Services and International units scanned email message storage areas on Microsoft Exchange Servers company-wide to eradicate infected emails. Approximately 24 Nimda infected emails were identified and deleted.
- **Trend Patterns** - Trend patterns that detect Nimda infected emails were deployed on late on Tuesday morning (9/18) on Exchange servers and on email interfaces to the Internet. Rapid deployment of anti-virus detection prevented a mass distribution of infected emails throughout the system during mid-afternoon on 9/18.
- **NAV Definition Deployment** - An initial set of NAV definitions were deployed late on Tuesday 9/18. A second set of 9/18 definitions that detect several new variants was deployed during mid-day on 9/19. ALL BUSINESS units asked to verify that current NAV definitions are active on desktops and remote computers. NAV definitions dated 9/24 were scheduled for deployment in-line with the normal weekly deployment on 9/27.
- **Instructions To Report Nimda Infected Systems were developed and distributed** - Report infected Nimda systems to the Global Network Operations Center (GNOC) using instructions

- **Instructions For Identifying Nimda Infected Systems were developed and circulated** - Please follow the link Security supplied infection identification instructions

- **Procedure for Remote Users were developed** - In order to protect remote user systems from the NIMDA worm, it is imperative that Remote users update their Norton AntiVirus definitions to the 9/18 (or higher) by either of the following methods:
    - For NAV 2001(employee home machines) connect to the Internet, run Live Update when you are
    - For other versions of NAV, follow your business units instructions or:
    - Download current updates from: http://www.sarc.com/

- **Internet Explorer Browser Use Policy was updated and circulated** - Restrictions on Internet Explorer use is being lifted by business unit based on full deployment of NAV dated 9/18 (or higher) and the degree of IE Mime Vulnerability patching done in each business unit. A list of business units that have approved IE use is posted on: http://alert.xxx.xxx

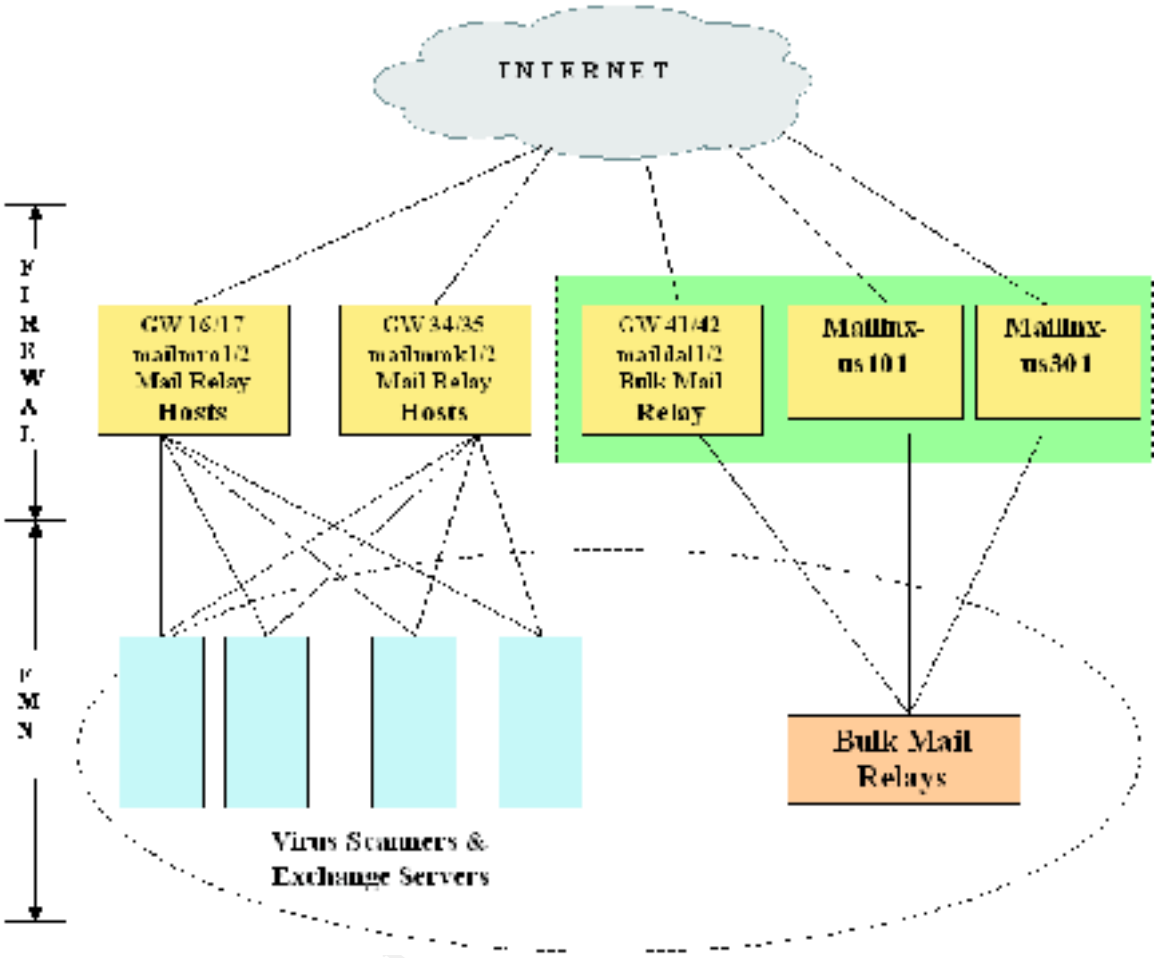
To handle the virus incidents (in this case Nimda.a as well as Nimda.e) the following plan was used for the virus incident handling and response team:

#	Task	Responsible	Start	End	Comments
1.	Become aware of new virus threat, conduct research (Trend, Symantec, F-Secure, IBM-ERS, REACT, SANS, Kumite.com), evaluate severity	Internet Security team (ISSG) Contact: XXX			Is there a detect/fix? - Symantec - Trend
2.	Notify Security Services Command Center (BCC)	ISSG			Call xxx-xxx-xxxx
3.	Page ISSG_VIRUS_ASSESMENT group via Change mgmt. System (PACE) using pre-defined text. MANUALLY call others onto the bridge: UK Data Center (x-xx-xxxx), JFC (Far East), CSC, DCO, Command Ctr	BCC, CSC, or DCO			"To Virus Assessment Team from CVD: Please join virus assessment bridge at xxx-xxx-xxxx ID# xxxx"
4.	Call into bridge	Team Members			
5.	Review incident to date & potential impact	ISSG & Team			
6.	Open PACE problem ticket at severity 1 or 2; assign ticket to ISSG	CSC			Ticket # =
7.	Determine if advisable to take immediate action: queue Internet email bring down inter-site X.400 connectors block email with certain subjects via eManager or ScanMail	ISSG & Team			Allows time to assess and respond
8.	Queue domestic Internet mail	ISA			
9.	Queue International Internet mail	External international Firewall			
10.	Bring down inter-site X.400 connectors	MSS			
11.	Review predefined action plan and modify if needed (e.g. don't alert end-users or accelerate	ISSG & Team			

#	Task	Responsible	Start	End	Comments
	normal process)				
12.	Notify Mgt & of analysis, actions taken & action plan	Each Team Member			
13.	**Action Plan:** **(tasks 14 – 42)**				
14.	Decide if advisable to "warm up" the Corporate EOC. If so, BCC notify CCP on call.	Team			
15.	Review/Modify "Heads-Up" Tech Message	FSSI M&C			Info about the threat. "Be prepared to respond"
16.	Review/Modify End-User Messages for multiple media: Email (FNI Regular dist or special) Web sites (alert.xxx.com, xxx, issg) Voice mail SYMON Boards Newsline Door Posters Remote Access Gateway Banners	FSSI M&C			"A new virus has been discovered named VVVV. Don't open emails titled ZZZZ", etc.
17.	Post "Heads-Up" Tech Message on 800 Status Information Line	CCP			
18.	Page Information Security Officers of each Business groups (ISO's), VRTs & others with 800 Status Information Line PACE groups	FSSI Boston Security Console, CSC or DCO			Text: "Call the info line at 800-xxx-yyyy for information about a virus threat."
19.	Send message via e-mail	Corporate Communications, DIS, or MSS			
20.	Send message via voice-mail to employees	Voice Engineering			
21.	System Monitoring (SYMON) board update	CSC			
22.	Apply Remote Access Gateway Banners	RMS, NEVIS, xxxx			
23.	Apply Posters to all main entrances and office doors	FSSI Ops			
24.	Get sample of virus if possible	ISSG			
25.	Test current antivirus tools in lab to see if effective soln is effective	ISSG			NAV Trend ISVW
26.	Download definitions from Symantec if necessary	ISSG			Def. Date = # of Viruses =
27.	Download patterns and engine updates from Trend if necessary	ISSG			Pattern # = Engine =
28.	Test downloaded antivirus definitions/patterns/engines in lab to see if effective	ISSG			Symantec Trend
29.	Copy definitions/patterns/engines to FTP server test directory and notify DS, MSS	ISSG			Symantec Trend
30.	Notify DCO to ignore stopped service alerts on Trend ISVW servers under PACE ticket# while patterns/engines are being updated. Provide estimated completion time for updates.	ISSG or MSS			
31.	Update ISVW pattern (and engine if needed)	ISSG			

#	Task	Responsible	Start	End	Comments
	on four domestic servers				
32.	Update ISVW pattern (and engine if needed) on two international servers	Lan Admin group			
33.	Notify DCO to resume monitoring Trend service on Trend ISVW servers	ISSG			
34.	Monitor mail flow for abnormalities for 5 minutes	MSS			
35.	Pilot NAV install on desktops	DS			
36.	Update ISSG Web pages http:/www.xxxx.xxx.xxxx	ISSG or FSSI M&C			Include Trend ISVW status on new virus or alert page(s)
37.	SMS distribution of NAV definitions	DS & NEPS			
38.	Update Bulletin with new virus information, URL to download definitions, and SMS distribution information. Post on DS web page. Distribute link to Desktop System Planning Team and LAN Admins.	DS & ISSG			
39.	Send Bulletin or link to a. ISO's and Advisors b. VRT's and interested parties.	ISSG			
40.	Update Intranet Web Site with new NAV definitions	Site-manager			
41.	Discontinue Employee Communications - remove door signage - remove SYMON board messages - remove web site alerts - remove remote access gateway banners	FSSI			
42.	Close PACE Ticket	ISSG			

Diagram of the Mail Server configuration:



Here are the steps that were taken for identification and reporting on the incident, eradication and then recovery process:

A. INSTRUCTIONS FOR REPORTING NIMDA INFECTED SYSTEMS

Desktop Issue

- Customer calls **their** Help Desk.
- Help Desk has customer disconnect LAN cable, obtains IP address & Machine Name
- Help Desk calls ICS @ (xxx) xxx-xxxx, to disconnect port. Rep provides Ip address, Machine Name and ticket #
- HD opens PACE ticket to local Desktop team

- Desktop repairs virus, certifies cleaning and sends ticket to ICS for port to be re-enabled and ticket to be closed.
  (ICS has the ability to view FRIS TECHLINE, FIRSCO Helpdesk & TSS formats, as well as the CSO, Device & Network categories).

Server Issue

- Admin or Help Desk calls ICS @ (xxx-xxx-xxxx, to disconnect port
- ICS disconnects port, transfers or calls CSC to have ticket opened to Swat team.
- CSC opens tickets and calls ABC @ xxx-xxx-xxxx
- Swat team has server cleaned and certified, and sends ticket back to ICS to have port re-enabled.

A. INSTRUCTIONS TO DETERMINE IF A SYSTEM IS INFECTED WITH THE NIMDA WORM

Please check the following list to determine whether an NT or Win2K server is infected with the W32.nimda worm.

The following files and actions are listed in the likely order that the worm creates them.

- Does admin.dll exist anywhere that it has a size of 56 bytes (c, d, e drives)
- Does guest account exist for the local admin group
- Does readme.exe file exist anywhere
- Do any files exist named tftp followed by any number of digits (e.g., tftp2343)
- Does mmc.exe exist in the /winnt directory

If none of these exist then it is reasonable to conclude that the server is not infected.

Then please ensure that the server is patched against the following vulnerabilities.

Microsoft Security Bulletin MS00-057
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms00-057.asp

Microsoft Security Bulletin MS00-078
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms00-078.asp

Microsoft Security Bulletin MS01-020
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-020.asp

Microsoft Security Bulletin MS01-033
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-033.asp

At a minimum the all of the patches listed above must be applied to your server before putting it back into service.

If possible the Security Rollup Package should be applied to the server to insure full compliance.

Microsoft Post-Windows NT 4.0 Service Pack 6a Security Rollup Package (SRP)
http://support.microsoft.com/directory/article.asp?ID=kb;en-us;Q299444

NOTE: All patches should be tested before applying to production servers.

B. STEPS TO FOLLOW PRIOR TO RETURNING NT/WIN2K SYSTEMS TO THE NETWORK

Check the following list to determine whether the server is infected with the W32.nimda worm.

The following files and actions are listed in the likely order that the worm creates them.

- Does admin.dll exist anywhere that it has a size of 56 bytes (c, d, e drives) ?
- Does guest account exist for the local admin group ?
- Does readme.exe file exist anywhere in the file system ?
- Do any files exist named tftp followed by any number of digits (e.g., tftp2343) ?
- Does mmc.exe exist in the /winnt directory ?

If none of these exist then it is reasonable to conclude that the server is not infected and should now be patched against the vulnerabilities listed below.

If any of the above conditions exist perform the following:

Note: Once a computer has been attacked by W32.Nimda.A@mm, it is very difficult to determine what security settings have been compromised. Unless - by reading the logs - you can be absolutely sure that nothing else malicious has been done to the computer, it is best to completely reinstall the system. This is the only way you can be 100 percent certain that the computer is clean.

1. Install the latest Norton AntiVirus definitions.
2. Locate the line that begins with Shell= in c:\windows\system.ini. Remove all text following Explorer.exe from this line. When finished the line should look like:

   shell=Explorer.exe

   Note: If Windows is installed in a different location, make the appropriate substitution. Also, some computers may have an entry other than Explorer.exe after shell=. If this is the case and you are running an alternative Windows shell, then change this line to shell=Explorer.exe for now. You can change it back to your preferred shell after you have finished this procedure.

3. If AutoProtect is not enabled, enable it before restarting the computer. For instruction on how to do this please read the document How to enable and disable NortonAntiVirus Auto-Protect
   http://service1.symantec.com/SUPPORT/nav.nsf/396b6ccde72d4a4d882569fc006071d4/84953e4d6ab65f54882565600074b968?OpenDocument>.
4. Restart the computer.
5. Start Norton AntiVirus (NAV), and make sure that NAV is configured to scan all files. For

instruction on how to do this, read the document How to configure Norton AntiVirus to scan all files http://service1.symantec.com/SUPPORT/nav.nsf/docid/1999110513272906.
6. Scan your system with NAV. For instruction on how to run a scan with NAV, please read the document: How to scan for viruses http://service1.symantec.com/SUPPORT/nav.nsf/docid/2001050909295006.
7. For each file detected as infected by W32.Nimda.A@mm or W32.Nimda.A@mm (html), choose Repair.
8. For each file detected as infected by W32.Nimda.A@mm (dr), W32.Nimda.enc, W32.Nimda.A@mm (dll), choose Delete.
9. Restore admin.dll and riched20.dll from backup or the Windows/Office .cab files if necessary.
10. Remove unnecessary shares.
11. Delete the guest account from the Administrators group (if applicable).

Then ensure that the server is patched against the following vulnerabilities.

Microsoft Security Bulletin MS00-057
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms00-057.asp

Microsoft Security Bulletin MS00-078
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms00-078.asp

Microsoft Security Bulletin MS01-020
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-020.asp

Microsoft Security Bulletin MS01-033
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-033.asp

Microsoft Security Bulletin MS01-044
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-044.asp

At a minimum the all of the patches listed above must be applied to your server before putting it back into service.

If possible the Security Rollup Package should be applied to the server to insure full compliance.
Microsoft Post-Windows NT 4.0 Service Pack 6a Security Rollup Package (SRP)

http://support.microsoft.com/directory/article.asp?ID=kb;en-us;Q299444

[Caution this package exposes an issue with versions earlier than 4.24.0.0 of the Compaq Array Controller device driver (Cpqarray.sys). Proceed only after testing in a non-production environment]

NOTE: All patches should be tested before applying to production servers.

C. INSTRUCTIONS TO RECONNECT A PREVIOUSLY NIMDA INFECTED TO THE NETWORK

To regain network connectivity:

1. After your computer has been patched and NAV definitions are updated
2. Close PACE Ticket and Assign to PACE Group ICS. (If you need assistance with this process, call CSC 1-800-xxx-xxxx, Option #2)
3. Call into the event bridge at 1-xxx-xxx-xxxx, ID# xxxx, Break out 3 (push #, 1, 3) and request reconnection.

Lessons Learned.

1. Apply Security patches in time and ensure all the systems in the organization comply with the latest patches from virus vendors as well as from o.s. vendors. The main reason why we got hit in a big-way was many of the developer used Microsoft PWS web server on their desktop and had not applied the latest patch, became victim of the attack and subsequently affected others.
2. Scanning all the servers on a regular basis to ensure latest patches are applied and working.
3. Enforce system policies (such as Internet browser use policy) via constant monitoring and reporting.
4. Constant preparation, education and awareness are the key to the success in prevention, containment and eradication of Cyber incidents.

References:

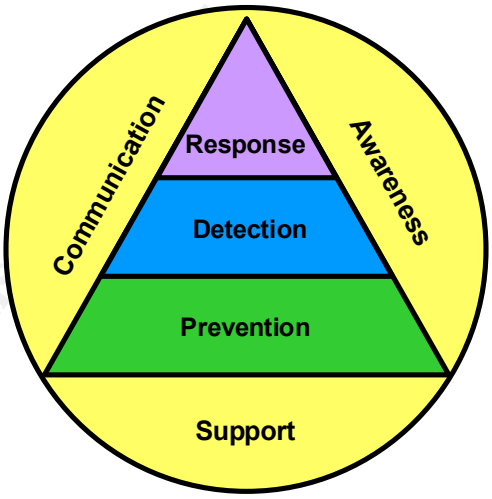
- CIAC (Computer Incident Bulletins): http://ciac.llnl.gov/cgi-bin/index/bulletins
- CERT (Computer Emergency Response Team) Advisories: http://www.cert.org/advisories
- CERT (Computer Emergency Response Team) Vulnerabilities: http://www.cert.org/vul_notes
- CERT (Computer Emergency Response Team) Reported Incidents: http://www.cert.org/incident_notes
- **Symantec:** http://www.sarc.com/avcenter/venc/data/w32.nimda.a@mm.html
- **Trend Micro:** http://www.antivirus.com/vinfo/virusencyclo/default5.asp?VName=PE_NIMDA.A
- **Technical Analysis (SANS):** http://www.incidents.org

References and material used in this article is also from:

- **Nimble Nimda Numbed My Network! Submitted By Stacey A. Swart to SANS practical exam**.
- **W32/Nimda.A.mm Worm Analysis Practical Submitted by: Christine Vecchio-Flaim for SANS practical exam**
- **Our company's web Site on security and cyber incident handling process.**

Annexure 1

Cyber Security Incident Response Business Unit Guidelines



Internal Information
Revision Date: xx/xx/xx

For other Cyber Security Incident Response Information please visit our website at:
http://xxx.xxx.com /cyber/index.html

1.0 Introduction

1.1 Overview

The company ABC (henceforth referred as the company) relies heavily on computer processing and associated computer technologies to support critical business functions. Even a short service interruption of this type, due to a cyber information security incident, could significantly and adversely impact customer relations, business operations and/or Company's reputation. The threats are real and growing due to the following:

- *Rising Use of Electronic Commerce*: The 1998 Computer Security Institute/FBI Information Security Study reports that the number of organizations that use the Internet for electronic commerce rose to 30%. Electronic commerce plays a major role in Company's marketing and information processing strategy. Internet connectivity provides an attractive conduit for potential exploitation from outside sources.
- *Increasing Internet Attacks*: The same study cites that companies reporting the Internet as a frequent point of attack rose from 37% in 1996 to 57% in 1998.
- *Threats*: The scope of potential perpetrators and their level of technical expertise are continually increasing. Now hackers, industrial spies, computer warriors, cyber terrorists, etc., are major concerns.
- *Technological Improvements – Technology has become cheaper, more powerful and generally more available to people who might exploit computer systems.*
- *Availability of Hacker Tools*: A wealth of hacker sites and hacking resources are generally available on the Internet.
- *Internal Abuse*: The CSI study also points out that unauthorized access by internal users rose for the third straight year to 55%. This information underscores the fact that a majority of computer based abused is committed by internal employees even though external system penetrations tend to draw the largest amount of cyber incident attention.

For these reasons there is a substantial need for a coordinated Company corporate level and Business Unit incident response capability.

1.2 Goals

The overall goals of these Business Unit Cyber Incident Response Guidelines are to:

- *Develop Guidelines That Work For All Business Units*: - These Guidelines must be specific enough to guide Company Business Units in cyber incident process development, yet be general enough to be applicable to all Business Units.
- *Answer "What would we do if?"* The overriding question Company Business Units need to answer is, "What would we do if we had a cyber incident?"
- *Define Qualifying Cyber Incidents*: Business Units need to know what cyber incidents are, which ones qualify under the Program and how to recognize them.

- *Identification, Verification, Escalation & Reporting*: Cyber incidents are an increasing concern and awareness needs to be raised to facilitate identification, verification, escalation and reporting of cyber security events to the corporate level.
- *Define Business Unit Roles & Responsibilities*: These Guidelines will help each Business Unit to define its cyber incident roles and responsibilities model.
- *Inform Business Units of the Corporate Level Process*: The Guidelines let Company Business Units know basic information about the corporate level process and how they should interface to and interact with it.

2.0 Understanding Cyber Incidents

2.1 Overview

Identifying cyber incidents is of critical importance in the incident response process. However this is a significant challenge given rapid changes in technology and the seemingly unlimited ability of potential perpetrators to think of new ways to exploit vulnerabilities in computer systems and networks.

2.2 What Is a Qualifying Cyber Incident?

In general terms, a cyber security incident is an actual or potential misuse, exploitation or unauthorized penetration of Company's information technology infrastructure. That infrastructure includes Company's computer systems, networks, applications (including information conduits where Company information is being transmitted to or from Company), PC/LAN environments, etc.

2.3 How to Recognize A Cyber Incident

In general, four things are critical in recognizing cyber incidents. First, Business Unit technical support, program development, security and the general user communities must to be aware that cyber incidents can be a serious problem. Second, those people need to be suspicious of unusual system/security activity. Third, system/security administrators must to do the security basics well e.g., reviewing system/security logs, generate/review security violation reports, etc. Fourth, action needs to be taken to increase intrusion detection alerting and reporting of unusual system activity throughout Company.

More specifically, there are cyber incidents that individual system users need to be aware of and ones that security/system administrators would typically see. Some examples of possible cyber security incidents that individual users might notice are, but are not limited to:

- *PC Tampering*: Some situations may indicate that someone has attempted to gain unauthorized access to a PC/laptop/handheld computer or to tamper with the integrity of the hardware to gain access to information on the unit or to Company's network.
- *Unauthorized Access to Restricted Company Information*: Evidence may indicate that an attempt(s) has been made or actual unauthorized access(es) has been gained to restricted Company information resources on any Company computing platform. For example, it appears that someone gained unauthorized access to sensitive (Human Resource, insider trade information, restricted marketing, financial transaction, etc.) files residing on a Company computing platform.
- *Internet Abuse*: Company employee activity on the Internet that is outside of that allowed in the Company Corporate Conduct Policy regarding Electronic

Communications Usage. For example, breaking into a competitor web site or sending forged email.

- *PC Controlled Remotely*: It is possible for software to be loaded to a PC remotely, which allows the remote user full control of the target machine. Two examples are NetBus (NT) and Back Orifice 2000 (NT & Windows 95/98).

Some examples of possible cyber incidents that a system or security administrator might notice are, but are not limited to:

- *Intrusion Detection*: Alerts that are initiated by intrusion detection software indicating that a computer system or the network might be under attack by an unauthorized users(s).
- *Suspicious System/Security Log File Activity*: Computer system, security or other critical log/tracking files may indicate that unauthorized activities might be occurring on a Company computer system.
- *Missing or Altered System/Security Log Files*: System or other critical log/tracking files may be missing or altered, which might indicate that an authorized or unauthorized user(s) is trying to cover-up unauthorized activities.
- *Unauthorized Internet/Intranet Web Site Manipulation*: Reports that a Company Internet/Intranet web page has been defaced/altered.
- *Abuse of High Level Privileges*: Security logs indicate unexplained use or abuse of "root", "Administrator" or other similar high level access.
- *Suspended User IDs*: An inordinate number of suspended user accounts might indicate that someone had tried to guess user passwords or ran an automated password guessing tool against your system.

3.0 The Business Unit Process

3.1. Overview

The objective of this section is to aid Company Business Units in designing and developing a process to handle cyber incidents up to the point where the Corporate Security Cyber Incident Team needs to be contacted and the Corporate Level Process initiated. Additionally, Business Unit contacts involved in the cyber incident response process need to be aware of their continued involvement in conjunction with Corporate Security through the remainder of the cyber security incident.

An overview of the specific steps that your Business Units need to take in this process are:

Step 1 *Organize a Cyber Incident Process Development Team Meeting(s)* - Determine appropriate Business Unit representatives and possibly others to be involved in developing the Business Unit Cyber Incident Response Process. (*Responsible*: The Business Unit Information Security Officer).

Step 2 *Conduct a Cyber Incident Process Development Meeting(s)* – Conduct a meeting (s) to develop the Business Unit Cyber Incident Response Process and any additional meetings if needed. (*Responsible*: Business Unit Information Security Officer).

Step 3 *Appoint Business Unit Cyber Incident Contact(s)* - Establish your Business Unit's liaison to Corporate Security in the event of a cyber incident. (*Responsible*: The Business Unit Cyber Incident Process Development Team). Next, notify Corporate Security of the liaison(s) right away including their contact information. (*Responsible*: The Information Security Officer). The default/backup is the Business Contingency Planner.

Step 4 *Develop the Business Unit Cyber Incident Response Process* - Develop the Business Unit Cyber Incident Response Process to facilitate Business Unit cyber security incident verification, escalation and reporting to Corporate Security. After completion, the process should be reviewed and approved by the ISO and appropriate level(s) of Business Unit Management. Also, this process should be integrated with other Business Unit operational and response processes/procedures. (*Responsible*: The Business Unit Cyber Incident Process Development Team).

Step 5 *Notify Corporate Security* - Let Corporate Security know that you've completed development of your Business Unit's Cyber Incident Process. (*Responsible*: The Business Unit Information Security Officer).

Step 6 *Increase Awareness* - Facilitate understanding of your process and how it relates to the Corporate Level Process within your Business Unit. (Responsible: The Business Unit Cyber Incident Process Development Team).

In the following section, 3.2. Process Development Steps (Expanded) is an expanded view of each step in the Business Unit Cyber Incident Response Development Process.

3.2. Process Development Steps (Expanded)

This section expands each step in the Business Unit Cyber Incident Reponse Development Process outlined in section 3.1.

It is important to note that Business Unit cyber incident processes only apply to cyber incidents that occur on platforms (PCs, LANs, networks, servers, mid-range, mainframes, firewalls, etc.) and applications for which their Business Unit has operational responsibility. For instance, a Business Unit may be the "owner" of web servers, which are administered operationally by a Company service organization (e.g. Systems Company). In this situation, the web server "owner" doesn't have responsibility for having a cyber security incident response process in place, but the Company computing service organization does. It's recommended that Business Units verify that their computing service organizations (internal or external) have a cyber incident response process in place.

3.2.1. Step 1: Organize a Cyber Incident Process Development Team Meeting(s)

The Information Security Officer (ISO) is responsible for coordinating cyber incident process development at the individual Business Unit level. To do this, the ISO needs to gather the right people within their business to develop the process. To facilitate identification and representation of the proper functions in this process, a list of required, recommended, and optional representatives and their associated responsibilities are detailed below:

- *Information Security Officer (ISO)*: Is responsible for initial and on-going coordination of the Cyber Security Incident Response Program (REQUIRED).

- *Business Contingency Planners (BCP)*: The contingency planning experience of Business Unit BCPs can be leveraged by the Process Development Team. Additionally, the BCPs may have additional responsibilities as an initial Business Unit information contact for Corporate Security. (RECOMMENDED).
- *Technical Support*: These groups require representation to verify the computing platforms that the Business Unit is responsible for and need to contribute input if operational procedures need to be developed for cyber incident identification, verification and resolution. (REQUIRED).
- *Application Development/Production Support*: This group(s) should contribute input to the operational Business Unit procedures due to their roles in cyber incident identification, verification and resolution. (REQUIRED).
- *Computer Operations Support*: This group(s) needs representation due to their potential roles in cyber incident identification and resolution. (REQUIRED).
- *Information Security Administration*: This group(s) needs representation due to their roles in cyber incident identification and resolution. This role is likely to be filled by a BISD, BISS, ITSD, ITSS or Security Administration Manager. (REQUIRED).
- *Business Unit Help Desks*: If available, may play a role as a conduit for Business Unit cyber incident escalation process. (RECOMMENDED).
- *Risk Managers*: May need to be involved in representing the Business Unit viewpoint on cyber incident risks (RECOMMENDED).
- *Virus Response Team (VRT) Members*: The incident response experience of Business Unit VRTs should be of use in the Cyber Incident Process Development Team (RECOMMENDED).

3.2.2. Step 2: Conduct a Cyber Incident Process Development Meeting(s)

Each Information Security Officer is responsible for coordinating a Cyber Incident Process Development Meeting to bring together the Business Unit's people who are the focal points for:

- Identifying/detecting potential cyber incidents.
- Verifying them as cyber security incidents, if necessary.
- Outlining the process for escalating them within your Business Unit
- Reporting them to Corporate Security.
- Working with Corporate Security to provide additional support (technical, programming, information security, etc.) in resolving the reported incidents.

3.2.3. Step 3: Appoint Business Unit Cyber Incident Contact(s)

In the Cyber Incident Process Development Meeting, team members need to determine the best liaison to Corporate Security for their Business Unit in the event of a cyber security incident. The requirements for this role are:

- Must supply 24x7x365 Availability via cell phone or pager.
- Will assemble appropriate Business Unit management, technical, security, and computer operations representatives for Corporate Cyber Incident Response meetings or conference calls.

- Will act as the liaison for Corporate Security communications to and from the Business Unit.
- Will oversee and report on progress of the Business Unit's cyber incident response resolution efforts to the Corporate Cyber Incident Team .
- Must maintain a confidential posture for all cyber incidents and related issues.
- Must provide backup support when the primary support person is unavailable.

Potential individual(s) to support this responsibility are the Information Security Officer, Risk Manager, Technical Support manager, Business Contingency Planner or other qualified Business Unit representative.

Once the contact is determined, the ISO needs to send an email to the "Corporate Cyber Incident Response" mailbox naming the Business Unit Cyber Incident Contact (and backups) and their contact information. The contact information should include work, home, pager and cell phone numbers.

Corporate Security will maintain a list of these Business Unit contacts, but the Business Unit's are responsible for providing changes in contact information to Corporate Security on a timely basis.

If a contact person is not assigned or is unavailable, the default "initial" contact will be the Business Contingency Planner due to the BCP's 24x7x365 availability and knowledge of Business Unit contacts. Then, the BCP would designate other contacts to be referenced throughout the remainder of that cyber information security incident.

3.2.4. Step 4: Develop the Business Unit Cyber Incident Response Process

This step is the main goal of the Cyber Incident Process Development Meeting(s), which is to design a process that facilitates cyber incident identification, verification, escalation within the Business Unit and reporting to the Corporate Level.

Please note that all Company Business Units are required to report qualifying cyber incidents to Corporate Security for assessment and possible Corporate Level handling.

3.2.4.1.Pre-Corporate-level Reporting Steps

The Business Unit Cyber Incident Process needs to be designed based on three basic steps:

- *Identification*: Business Units and Corporate Security can't provide timely and effective cyber incident response actions unless potential cyber incidents are identified. In the short term, the best way to do this is to raise awareness to let system users, computer operations staffs, application development, security/system administrators, etc., know to be on the lookout for unusual activities, like those things mentioned in section 2.2: Recognizing A Cyber Security Incident. In the long term, network and host-based intrusion detection software needs to be put in place if it's not in place yet and the effectiveness of these systems needs to be increased.
- *Verification*: Once initially identified, certain cyber issues require little verification to confirm that they are in fact cyber security incidents (an Internet/Intranet web site has been defaced, etc.). Those issues

should be escalated within the Business Unit and reported to Corporate Security immediately.

Other cyber issues require verification by the Business Unit Information Security Administrators, Computer Operations or Technical Support Staffs, etc., to confirm that they are not a result of operational, system performance, security administration, etc., problems. For instance, preliminary Business Unit review might determine that a legitimate system problem resulted in log records not being recorded in a system or security log file, e.g., a hacker didn't delete them.

If the issue still looks like a cyber security incident after the review, then the issue should be escalated as a cyber incident within the Business Unit.

- *Escalation*: It is recommended that Business Units escalate cyber incident reports through a central group (help desk, emergency operations center, etc.) where the event can be documented manually or by using a prescribed Business Unit ticketing system. Next, the central group can notify the Business Unit's Cyber Incident Contact (ISO, Risk Manager, BCP, etc.), who in turn is responsible for contacting Corporate Security.

Also, after developing the base process, the Business Unit Cyber Incident Process Development Team needs to consider if additional computer operations, applications, programming/development, information security, etc., procedures need to be modified or developed to encompass cyber incident considerations. For instance, intrusion detection procedures may need to be modified to document the cyber incident connection. These procedures and the Business Unit Cyber Incident Response Process must be periodically reviewed to keep them current.

Cyber incidents are, at a minimum, to be treated as "Company Confidential" events. It is recommended that the process reflect that all individuals involved in the response effort treat all incident information, conversations, inquiries from outside sources, etc., in accordance with that classification. For more information on information classification please reference Corporate Security's web site at http://xxx.xxx.com/security/spi .

3.2.4.2.Assign Business Unit Process Roles & Responsibilities

Next, roles and responsibilities for the Business Unit Cyber Incident Response Process need to be assigned. To facilitate incident response assignments in support of the Business Unit Cyber Incident Response Process, the following list of required, recommended and optional roles and associated responsibilities are suggested:

- *Information Security Officer (ISO)*: At the discretion of the individual Business Unit, the ISO may have incident response responsibilities during tests and actual cyber incidents (OPTIONAL).
- *Business Contingency Planners (BCP)*: BCPs would need to respond to a cyber incident in the event of a business interruption. Also, BCPs may need to act as an initial Business Unit support contact for the Corporate-level response process. (REQUIRED).

- *Technical Support*: This group(s) may have technical identification, assessment and incident resolution tasks during actual incidents (REQUIRED).
- *Application Development/Production Support*: This group(s) may have technical identification, assessment and incident resolution tasks during actual incidents (REQUIRED).
- *Computer Operations Support*: This group(s) needs to contribute input to the operational Business Unit procedures due to their roles in cyber incident resolution support (REQUIRED).
- *Risk Managers*: At the discretion of the individual Business Unit, the Risk Manager may have incident response responsibilities during tests and actual cyber incidents (OPTIONAL).
- *BU Help Desks*: May play a role as a conduit for Business Unit cyber incident reporting, verification, tracking, escalation, etc. (RECOMMENDED)
- *Virus Response Team Members*: At the discretion of the individual Business Unit, the VRT may have incident response responsibilities during tests and actual cyber incidents (RECOMMENDED).

3.2.4.3.Corporate-level Reporting Steps

Next, cyber incidents that have been identified, verified and escalated within the Business Unit must be forwarded to Corporate Security. The Business Unit process needs to specify the Corporate Security escalation point. Specific Corporate Security contact information for cyber security incidents is as follows:

Business Unit incident reports should be made to the Corporate Security Evaluation & Response Line (E & R Line) at (xxx) xxx - xxxx

When calling the E & R Line, please be prepared to supply the following information:

- Your Name
- Your Badge number
- Your Business Unit
- The affected Business Unit
- The affected Department
- The location of the affected area
- Specific details of the incident
- Incident impacts
- Your contact information
- Any Business Unit contact information that is available

3.2.5. Step 5: Notify Corporate Security

After completing the development process and gaining Business Unit management approval, the Information Security Officer needs to send an acknowledgment of it's completion along with an electronic version of the Business Unit's escalation process to the "Corporate Cyber Incident Response" mailbox.

After receiving the Business Unit Cyber Incident Response Processes, Corporate Security will review them to ensure that they are in keeping with the intent of the Cyber Security Incident Response Program.

3.2.6. Step 6: Increase Awareness

To facilitate awareness of cyber incidents, how to recognize them and the Business Unit Cyber Incident Response Process, Business Units can take steps to "spread the word". Some simple methods for achieving this goal are:

- Update Business Unit Intranet web sites notifying users of the new process and contacts.
- Send an email notification to "key" Business Unit Management.
- Include an article detailing the new process in the Business Unit newsletter.
- Request that Incident Process Development Meeting Members brief their employees of the new process.

3.3. Expectations Of Business Units After Escalating To Corporate Security

In general, the need for Business Unit personnel participation for incidents escalated to Corporate Security tends to increase or decrease with the size, scope and impact associated with individual cyber incidents. That is, minor incidents may only involve very limited Business Unit Resources. Conversely, major incidents may require more extensive Business Unit resources. If Business Unit personnel are involved in a cyber incident response effort, any and all of the following expectations may be required at the direction of the Corporate Cyber Security Incident Response Team:

- Maintaining a timeline record of cyber incident events within Business Unit scope.
- Taking part in CSIR meetings or conference bridge discussions.
- Understanding technical and security issues associated with the incident.
- Assessing and communicating how the incident impacts business functions.
- Collecting and forwarding assessment information as required.
- Preserving and protecting data that is collected in case it is needed as evidence.
- Assessing response action steps and communicating the business impacts of proposed actions.
- Directing response action step implementation efforts within business unit scope.
- Supporting the response implementation efforts of other Business Units where possible and necessary.
- Adhering to guidance from the CSIR Management Team and/or the CSIR Coordinator and performing all requested actions in a timely manner.
- Informing the CSIR Management Team and/or CSIR Coordinator of significant events and reporting status on all assignments.
- Escalating issues to the CSIR Management Team and/or CSIR Coordinator for response or resolution.
- Providing a Business Unit support contact throughout the response effort.
- Participating in the incident post-mortem review process.

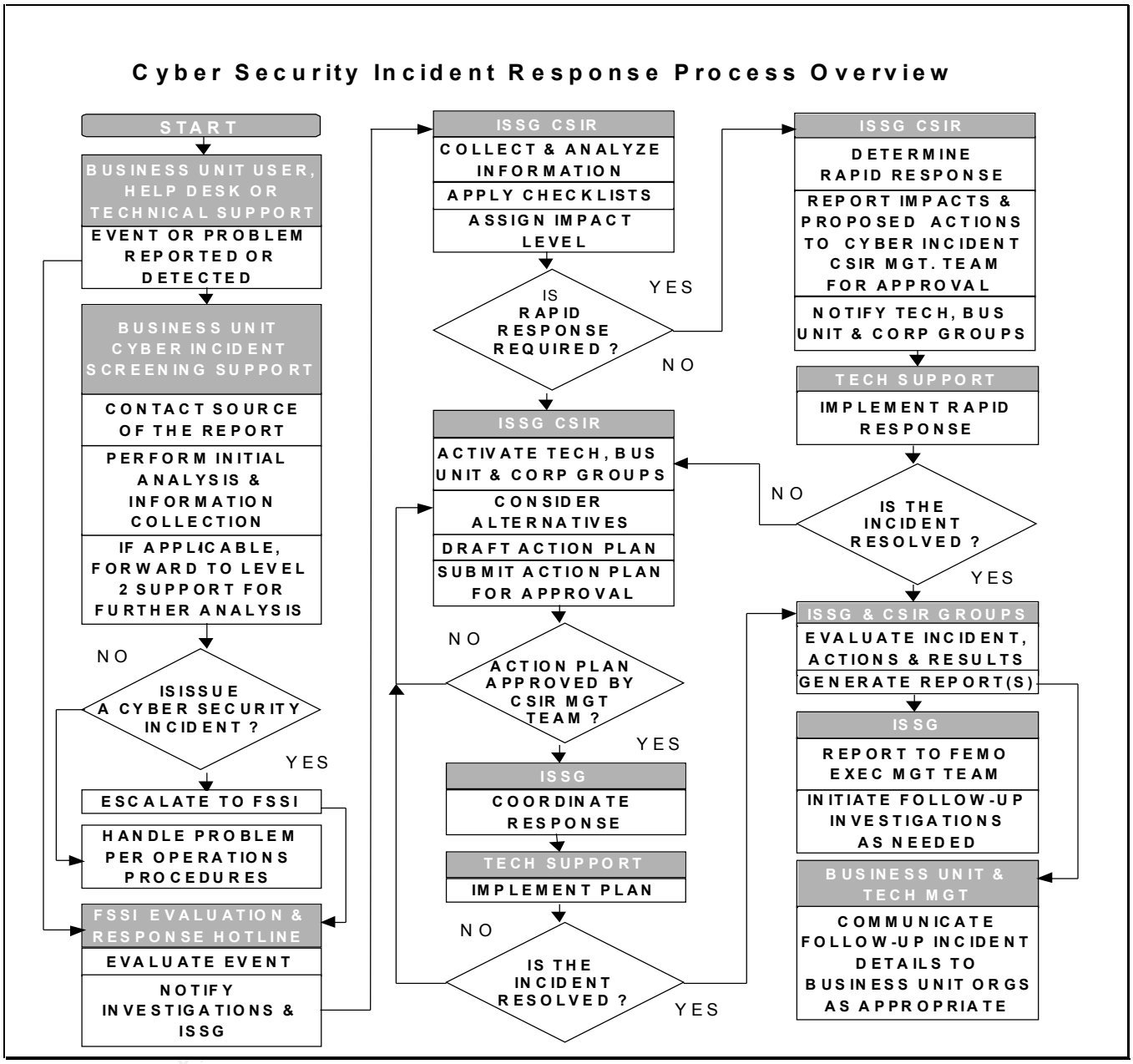
Business Unit management, technical, security, operations, etc. staffs should be made aware of these cyber security incident response requirements needed in support of a major cyber security incident.

4.0 The Corporate-level Process

4.1 Corporate Security Incident Response Handling Overview

In response to a Business Unit cyber incident report, actions are taken by Corporate Security correspond to the size and scope of the incident. The flowchart below illustrates the actions taken in the event of a major cyber information security incident and do not necessarily reflect the actions taken for every incident. It does, however, illustrate all of the basic steps in the process relating to identification, verification escalation, impact assessment, organization activation, rapid response, action plan development, management approval, response coordination, incident resolution, reporting and follow-up steps.

The Remainder of this page is intentionally left blank



4.2 The Corporate Cyber Incident Response Organization

The CSIR organization is comprised of cross-functional Company and non-Company resources that are assembled to assess significant cyber security incidents having varying impacts and to coordinate responses that may span multiple Company Business Units. The organization's role is to quickly mobilize various these resources in effectively responding to these incidents on a 24x7x365 basis.

The CSIR organization consists of The CSIR Management Team, a CSIR Management Team Leader, a CSIR Coordinator and three major Resource Groups: Technical; Business Unit; Corporate Services. The structure is designed for an appropriate level of Company Management

to provide incident handling and decision support during important or major cyber events. The Resource Groups provide analysis and hands-on incident resolution services. Additionally, the Resource Group Members may be called on to provide support services even if the Management Team isn't activated.

Please reference the following graphic and expanded CSIR organization explanation for a conceptual view of how the CSIR Organization is designed and how its component teams/groups relate to one another within the FEMO Executive Emergency Management Team framework.

**Reflects that only selected members may be involved when responding to an actual incident.*

4.3 Additional Corporate-level Support Elements

THE CORPORATE-LEVEL CYBER SECURITY INCIDENT RESPONSE PROGRAM ALSO PROVIDES FOR THESE ADDITIONAL SUPPORT ELEMENTS:

- *A Security Advisory & Vulnerability Service*: An important part of cyber incident response is to prevent incidents from happening in the first place. One major way of doing this is to ensure that system vulnerabilities noted from various sources are quickly rectified on Company's computing platforms. Also, security alerts help Company take actions to prevent potential threatening activity from outside of Company's computing environments. (This initiative will be underway in 2000).
- *Cyber Forensics*: Corporate Investigation Services provides robust investigation and forensic services.
- *"High-end" Cyber Incident Consulting*: This service can be used by Company to obtain "expert" cyber incident support in the event of a high severity incident.
- *Cyber Incident Checklists*: To help facilitate prompt and consistent incident response activities, checklists are used.

5. Appendix

Appendix A: Sample Cyber Security Incident Escalation Process

WHO	ACTION
Company Business Unit user, Help Desk, Computer/ Network Operations or Security Staff member.	❑ Reports a service interruption, suspicious system activity or intrusion detection alert to _____ at (xxx) xxx-xxxx. (*An appropriate Company Business Unit designated help desk or computer operations group.)*

Company Business Unit Help Desk, Computer Operations or Equiv Evaluation Group	❑ Initiates information collection via an applicable problem ticketing system or logs the event. (*Including: date; time; contact's name; badge number; Business Unit; Department; the problem; platforms/systems/applications effected; associate impacts; etc.)* ❑ Uses Business Unit incident handling procedures to attempt to determine if the incident is a qualifying cyber information security incident, i.e., not an operational, computer virus (*use normal virus contacts*), password or other issue not requiring a cyber incident response action. ❑ Level-two technical support group(s) assists in assessment of the problem and helps to verify it as a security incident, if necessary. ❑ If the issue is an operational, computer virus (*use normal virus contacts*), password or other issues not requiring a cyber incident response action, use normal operations procedures to report or resolve it. ❑ If the issue is a cyber information security incident report the event to the _____ _____ (*Business Unit Cyber Incident Contact*).
Business Unit Cyber Security Incident Contact	❑ Reports the event to Corporate Security as a cyber information security incident by calling the Evaluation & Response Line at (xxx) xxx-xxxx. ❑ Supplies the following information: ▪ Your Name ▪ Your Badge number ▪ Your Business Unit ▪ The affected Business Unit ▪ The affected Department ▪ The location of the affected area ▪ Specific details of the incident ▪ Impacts of the incident ▪ Your contact information ▪ Any Business Unit contact information that is available

** All Cyber incidents are, at minimum, to be treated as "Company Confidential" events. It is recommended that the process reflect all individuals involved in the response effort treat all incident information, conversations, etc., in accordance with that classification.

This page is intentionally left blank.

Annexure 2

FAQ For Employees on Cyber incident

- **What is a cyber security incident?**

  In general terms, a cyber security incident is an actual or potential misuse, exploitation or unauthorized penetration of within Company's information technology infrastructure. That infrastructure includes information residing on Company's computer systems, networks (including information conduits where Company information is being transmitted to or from Company), PC/LAN environments, etc.

  It is equally important to note that not all security related issues are cyber information security incidents. Security administration, operational, hardware, system performance, physical security, computer viruses, non-computer based (paper, mail, fax, cell phone, etc.) problems/issues are not addressed by the CSIR Program unless they were initiated by unauthorized activity. This is not to say that Corporate Security won't address these issues, but not using the CSIR Process. In particular, computer viruses are handled under the Corporate Virus Defense Program (http://xxx.xxx.xxx/issg/virus).

- **How would you know if you've been the victim of a cyber incident?**

  Cyber incidents are commonly detected by users of the computer system or by system/security administrators. Listed below are common cyber incidents that users or administrators might observe.

  Some examples of possible cyber security incidents that individual users might notice are, but are not limited to:

  - PC Tampering - An unauthorized attempt(s) to access or an actual access of a user's desktop or laptop PC.
  - Unauthorized Viewing, Copying, Updating or Destroying of Company Information - An unauthorized attempt(s) to view, copy, update or destroy Company information resident on a Company computing platform. For example, unauthorized viewing of confidential information or alteration of financial transactions residing on a Company computing platforms.
  - New/Unfamiliar Files – Individuals may notice that new files or unfamiliar files may exist in their directories or sub directories. This is sometimes an indication

that a Trojan Horse or some other nefarious process has been added to a file system.

Annexure 2

FAQ For Employees on Cyber incident

- PC Controlled Remotely – A user's PC may seem to be controlled from a remote source. This is sometimes an indication of the presence of remotely loaded software, which allows an unauthorized remote user to gain full control of a target machine. Some examples are NetBus (NT) and Back Orifice 2000 (UNIX & Windows 95/98).

Some examples of possible cyber incidents that a system or security administrator might notice are, but are not limited to:

- System Attacks - Alerts that are initiated by intrusion detection software indicating that a computer system or the network might be under attack by an unauthorized user(s).
- Missing or Altered System/Log Files - System or other critical log/tracking files may be missing or altered, which might indicate that an unauthorized user(s) is trying to cover-up his or her activities.
- Unauthorized Internet/Intranet Web Site Manipulation - Reports that a Company Internet/Intranet web page has been defaced/altered.
- Abuse of High Level Privileges - Security logs indicate unexplained use of "root", "Administrator" or other similar high level access.

- **I think that I have a cyber incident to report, what should I do?**

If your Business Unit has a procedure in place for handling cyber incidents, then use it. If you don't know what it is or you're not sure if your Business Unit has a procedure in place, please contact your Information Security Officer (ISO) (http://xxx.xxx.com/issg/isrc/iso-advlist.html). Otherwise, please call the Corporate Security Evaluation & Response Line to report the incident to the corporate incident response team at (XXX) XXX-XXXX.

- **What is the Cyber Security Incident Response (CSIR) Program?**

CSIR is a Company-wide Program designed to provide a prompt and coordinated process for responding to cyber incidents, which takes account of all business, corporate and technical impacts and solutions.

Independent studies show that computer system threats from outside (hackers, industrial spies, computer terrorists, etc.) and within (disgruntled employees, Internet abusers, unauthorized data access, etc.) businesses and organizations have grown

Annexure 2

FAQ For Employees on Cyber incident

---

substantially over the past few years. This Program is designed to address these risks.

- **Who is responsible for the cyber security incident response process at the corporate level?**

  Corporate Security (Company Security Services Inc.) is responsible for initiating maintaining and delivering the Program and its associated services. Within Corporate Security, cyber incidents are handled through a cooperative effort between Corporate Security's Investigation Services and the Information Security Services Groups.

- **Who is responsible for the cyber security incident response process at the Business Unit level?**

  The Business Unit level program is coordinated by each Business Unit's Information Security Officer (ISO) (http://xxx.xxx.com/issg/isrc/iso-advlist.html). The ISO is responsible for facilitating Business Unit efforts to institute a process that links computer operations/analysis functions to Corporate Security and Contingency Planning efforts.

- **What is an ISO?**

  ISOs are Information Security Officers. These are mostly Company Vice Presidents who represent their Business Unit President or Functional Head on the Information Security Risk Committee (ISRC), which meets once per month. The Information Security Services Group (ISSG) provides coordination of the ISRC of Corporate Security. ISOs are responsible for development and

delivery of the information security program for their business unit or function.

- **Who is my ISO?**

  If you want to find out who your Information Security Officer (ISO) is, please reference the ISO List (http://xxx.xxx.com/xxx/isrc/iso-advlist.html).

- **How does the Business Unit process relate to the corporate level process?**

  The Business Unit process is designed to interface with the corporate level process by assisting in identifying, verifying and

Annexure 2

FAQ For Employees on Cyber incident

---

escalating incidents within the Business Unit, then reporting them to the Corporate Security Cyber Incident Team. Please reference the Company Business Unit Cyber Incident response Guidelines (http://xxx.xxx.com/issg/cyber/guidelines.html).

- **What does Corporate Security do after a report has been received?**

  Corporate Security's Investigation Services and Information Security Service Groups analyze the issues and assign required FSSI resources to support the incident. Next, various parts of the pre-defined CSIR management, technical, Business Unit and Company corporate resources are activated, coordinated and an appropriate action plan are designed. Then, the CSIR Team works with appropriate Business Units to carryout the action plan(s) until the incident is resolved. Finally, Corporate Security provides incident follow-up activities and reporting as appropriate.

- **What other services does Corporate Security provide in support of cyber incidents?**

  In addition to basic incident handling, some of the other Corporate Security cyber incident support services include:

  - Business Unit Guidelines - Corporate Security supplies Company Business Units with guidelines to help them to develop a cyber incident process that interfaces with the corporate level process. Please reference the Guidelines at (http://xxx.xxx.com/issg/cyber/guidelines.html).

- Full-time Support - Corporate Security supports the CSIR process around the clock.
- Rapid Response - If needed, the CSIR process provides a rapid response capability to ensure that immediate initial action steps are taken.
- Cyber Forensics - Robust forensic support is provided to support cyber incident investigations.
- Law Enforcement Interface - Pre-established interfaces to appropriate law enforcement groups are available.
- "High-end" Vendor Support - Corporate Security has secured the services of a major incident response vendor to provide expert support in the event of a major cyber event.
- Security Advisory Services - In 2000, Corporate Security is planning to provide a Company tailored security alert and vulnerability advisory service. For more information on security advisories, please reference "What are Security alerts and vulnerability advisories?"

Annexure 2

FAQ For Employees on Cyber incident

- **How does contingency planning relate to Cyber Security Incident Response?**

  First, if a cyber incident causes a business interruption, then Business Contingency efforts may need to be invoked to restore business functions. Second, members of the Business Contingency Planning organization support the CSIR Program by providing "consulting" services in their areas of expertise, i.e., Legal, Corporate Communications, etc. Third, at an executive level, the CSIR process ties into the Company Emergency Management Organization.

- **What are security alerts and vulnerability advisories?**

  Various computer hardware/software vendors, information security organizations and government agencies issue vulnerabilities and alerts. Vulnerabilities typically deal with software design weaknesses that someone might try to take advantage of in attacking a computer system to gain access or a higher degree of access. These advisories usually specify how and where to obtain the "patch" (the fix for the exposure) and how to apply it.

  Alerts commonly involve fairly widespread and nefarious activity by hackers or people who distribute computer software "viruses". Viruses are programs that have the potential to damage computer systems or files and are typically spread through electronic mail. For more information on computer viruses please reference

Corporate Security's Virus Defense Web Site (http://xxx.xxx.com/issg/virus).

It is very important for system and security administrators to be aware of and to take action on security alerts and vulnerabilities to avoid potential system or security exploitations.

In 2000, Corporate Security is planning to provide a Company tailored security advisory and vulnerability service. Until then, security advisory and vulnerability links of some internal and external security groups are provided at (http://xxx.xxx.com/xxx/cyber/advisories.html).

- **How does the Computer Virus Defense Program relate to Cyber Security Incident Response?**

Corporate Security currently supports a Virus Defense Program, which pre-dated the Cyber Security Incident Response Program.

Annexure 2

FAQ For Employees on Cyber incident

Though viruses are technically a type of cyber incident, response efforts for cyber security incidents and viruses will continue to be handled separately until further notice.

End of Document