# Global Information Assurance Certification Paper

# Computer Virus Policy, Training, Software Protection and Incident Response for the Medium Sized Organization: A How-To Guide



SANS Security Essentials
Practical Version 1.2e

Chris Gullett
July 30, 2001

## INTRODUCTION

LoveLetter, Melissa, Navidad, SirCam, Code Red

– The names of computer viruses and worms have become headline news in the mainstream press. As they advance in technology and frequency, the cost to business has skyrocketed, from $7.6 billion[1] (US) in 1999 to $17.1 billion[2] in 2000. The addition of social engineering components to e-mail-delivered viruses and worms in the form of random subject lines and attachments makes user training more difficult[3]. The quick development and release of these viruses often catches system administrators and even anti-virus software vendors off-guard.

The need to minimize damage to systems and productivity requires a "defense-in-depth" strategy of policy, user training, software protection and virus incident response. While large corporations often have an information technology department and human resources infrastructure capable of implementing a multiple defense strategy, medium-sized businesses, schools and other organizations with several hundred users may find themselves in a more reactive than proactive mode when it comes to computer virus protection, detection and recovery.

This document outlines steps a medium-sized organization can take to create and implement a defense-in-depth strategy to protect resources against computer viruses.

## POLICY

The development of information systems security policies regarding e-mail usage and the use of software is the first step in our defense-in-depth strategy. The policy puts into written form the organization's emphasis on the proper use of e-mail and software installation; among the most common ways viruses arrive. An effective policy guides the development of standard operating procedures and helps transmit the importance of information systems security to the organization's computer users.

Your e-mail policy should include wording concerning virus prevention, such as:

> *E-mail attachments are one of the most common ways for destructive computer viruses to infect and damage your computer. Exercise extreme care when opening e-mail attachments. Never open an attachment when you are unsure of the source or the business-related reason the file is being sent. Always use the virus-scanning software provided on your computer. If you have any concerns about an e-mail attachment seek assistance from Information Systems before opening it.*

Your software policy should include similar language:

> *All software is scanned for viruses and subsequently loaded and/or distributed only after the product is shown to be free of viruses. This includes all initial loads as well as any upgrades or changes applied to the software.*

Special attention should be paid to the use of freeware and shareware.

Sample and actual security policies are readily available from dozens of sources on the Internet to assist you in you development of effective policies. Also available are books such as the Charles Cresson Wood's Information Security Policies Made Easy available from PentaSafe Security Technologies.

**USER TRAINING**

Ongoing user training plays an important preventative role in our defense-in-depth strategy to deal with computer viruses. Training takes three forms: 1) Group training sessions, 2) Training reminders, and 3) Reference material.

Group training sessions should be brief and interactive. They allow the organization to emphasize the importance of security polices, including the need to protect systems against computer viruses. More importantly, they allow end-users to ask specific questions about computer viruses and virus protection. In a medium-sized business, these meetings can be held by department and can be accomplished quickly. As users change and people forget, repeat these sessions at least annually.

Training reminders are regular memos e-mailed to users outlining the "best practices" of computer virus protection. Especially helpful are how-to tips on e-mail attachments or anti-virus software usage and virus definition file upgrades. When a major new virus is seen in the wild, such as the SirCam virus, use the opportunity to tie in news media coverage users may already be seeing with specific tips on avoiding viruses in your organization. For example,

> *Attention Computer Users!*
>
> *A new computer virus, W32.Sircam.Worm@mm, has begun to impact computer users around the world. The virus spreads easily through your e-mail account.*
>
> *The virus arrives as an attachment with random names and with random subject lines. It arrives in an e-mail from someone you know and both the subject line and attachment name may look like a normal business or personal e-mail message.*
>
> *Our e-mail anti-virus software has been updated and should intercept and delete this virus, however some users are receiving the virus*

*through personal e-mail accounts, such as those from Hotmail and Yahoo. These services are less secure than e-mail that passes through (your organization's) e-mail servers. The safest course is to never open attachments where you are unsure of the contents and/or the sender. This is especially important with this virus.*

*Infecting your computer from a personal e-mail account could lead to restrictions on accessing these types of accounts from our network. If you are a remote, dial-in, user please insure your anti-virus software is up-to-date.*

*Remember, you are an important part of our Security Policy. Please be sensitive to the issues involving viruses and how you can protect your computer and the network.*

*For more tips on avoiding computer viruses go to http://security.organizationname.com and select Virus Info from the menu.*

Thirdly, reference materials available on your organization's Intranet web site should round out virus protection training. (If your organization does not have an Intranet web site distribute written information on where users may find anti-virus information.) On-demand materials allow the end user to quickly access specific information on updating their anti-virus software and tips on preventing infections. Two particularly good examples of these types of materials are the Virus Primer[4] available from Trend Micro and the Anti-Virus Tips[5] available from McAfee. Another excellent tool to raise virus awareness among users is the Virus Information Updates tool[6] that can be added to your Intranet site's home page from Trend Micro.

**SOFTWARE PROTECTION**

Virus mitigation activities include keeping servers, workstations and other network devices up to date with security patches and service packs. Many infected systems result from the virus writer taking advantage of known vulnerabilities for which patches have previously been issued. Daily or weekly visits to the Vulnerabilities, Incidents & Fixes page at CERT[7] and subscribing to mailing lists such as those available from SecurityFocus.com[8] will provide vital information relating to security holes and available patches. Many vendors, such as Microsoft[9], also provide mailing lists and web pages dedicated to security vulnerabilities.

Even with properly updated systems, the computer user is clearly the first line of defense in preventing a virus infection. As virus creators build in more social engineering, users face lethal payloads disguised as games, pictures and memos from the boss. The majority of today's viruses would be avoided if computer users simply did not open unknown attachments. However, some viruses will invariably be

activated anyway, and the quality of your anti-virus software solution will be put to the test.

In most medium-sized organizations, at *least* two anti-virus solutions are required, a mail server and desktop/server solution. A good practice to follow is to use solutions from *different* vendors as on any new virus, one vendor may be faster to offer an updated definition file, or may be more accurate in detecting the virus. During the outbreak of the SirCam virus, for example, both Symantec (Norton) and Trend quickly provided updated definition files, but the Trend software did not detect the virus properly when it had certain attachment extensions, while Norton did identify and delete the virus. In other virus outbreaks the reverse has been true.

Occasionally overlooked in the mail server anti-virus solution is the sizing of the hardware involved. A significant outbreak can hit your mail server with hundreds or even thousands of infected e-mail messages in a very short period of time and an undersized server may become overloaded and allow infected messages to pass through.

If budget allows, a third layer of anti-virus protection may be added. Anti-virus software on your firewall or Internet gateway will increase protection, especially in light of the growing usage of personal, web-based e-mail accounts. Some vendors, such as SonicWall, now offer virus protection already built into their firewall products[10].

For the medium-sized organization, a desktop/server solution that offers centralized management is a must. Products such Norton Anti-Virus Corporate Edition[11] from Symantec and Trend's Virus Control System[12] allow for centralized management.

The case for centralized management is a strong one: If you have more than just a handful of computers, you cannot adequately insure your anti-virus solution is up-to-date. For a medium-sized organization with a few hundred computers, consider the time involved in rolling out updated virus definition files or scanning engine updates. Automatic updates via FTP and the Web pose a risky solution if there is no way to easily monitor if the update succeeded. Finally, anti-virus solutions that are not centrally managed may lack the components needed to alert administrators to a virus incident on a specific computer.

From Symantec's white paper Lower IT Costs through Better Anti-Virus Management:

> *… the standard architecture of AV products can cause serious delays, expenses, and loss of productivity for the companies who use them. Businesses need a new anti-virus architecture that can be modified, distributed, and installed quickly and cost-effectively when new classes of viruses are discovered.*

Centrally managed solutions reduce the staffing requirements needed while at

the same time offering superior updating and alerting features[13].

After choosing and installing your anti-virus solutions never overlook the need to test them. To facilitate testing in a production environment many anti-virus software vendors have agreed to recognize the test files from EICAR[14]. These test files are not actual viruses, but are designed to produce a positive response from anti-virus software.

## VIRUS RESPONSE TEAM

Unfortunately, there will come a time when a user injects a brand-new virus into a computer or network, one not yet detected by your vendor's anti-virus software. Whether the virus arrived on a floppy disk, via an e-mail attachment or through the exploitation of a server vulnerability, as happened with the Code Red worm, you are now faced with the immediate need to quarantine the virus, limit the damage to your information systems and find a resolution for both the infected machines and future protection.

The final part of our defense is a Virus Response Team. A very focused version of the more expansive Computer Incident Response Team[15,16] used by some large organizations, the Virus Response Team strictly deals with a virus incident that significantly impacts the medium-sized company's information systems. As such organizations often do not have sufficient information systems staff to fill all positions on the team, members may be drawn from other areas.

To develop a response plan, we first have to define when an incident is taking place and who will be in charge. A suggested policy to define when the team is activated would be:

> *The Information Systems Manager will designate primary and secondary staff members whose duties will include monitoring virus protection software and notifying appropriate personnel of apparent virus outbreaks. This monitoring must be done on a real-time basis using methods such as e-mail and paging.*
>
> *The declaration of a virus outbreak event is at the sole discretion of the Information Systems Manager or their designee* (note: the designee could be the primary or secondary monitors mentioned above)*.*
>
> *The decision to declare a virus outbreak event is subjective. Factors to be considered include the number of machines infected, users impacted, ability of the virus to spread and severity of the payload.*

Now that we have an idea of what defines a virus incident we can put together our team. The size of the virus response team should be in line with the number of users and resources for which the team is responsible. Information systems staff should be assigned so that there is a primary and secondary staff member assigned

to each role.

For a medium-sized organization with several hundred users, a suggested team plan includes the following members:

- Coordinator – Coordinates activities of the team, manages mail server and desktop virus solutions. Determines when resources must be shutdown or removed from the network. Briefs other departments and management on outbreak status as required. This should be your security administrator or a senior information systems staff member. This would also be the primary monitor mentioned above.
- Researcher – Responsible for researching the virus threat including payload, recovery options for infected machines and the status of vendor virus definition updates. This does not have to be an information systems staff member, but this team member needs to be a computer literate and very detail orientated.
- Mail Server Administrator – Responsible for reviewing mail server virus logs, determining which mailboxes may be infected, running any necessary removal utilities and suspending server operation at the request of the coordinator. Since most viruses now arrive via e-mail, this is an important position.
- Telecommunications – Responsible for establishing conference calls between as needed. Also notifies local users of virus information via public address and voice mail broadcast when necessary. This does not have to be an information systems staff member. It could be a telecommunications staff member or receptionist.
- Support Technician – Responsible for addressing server/desktop issues arising from a virus infection, including removal, and any data recovery services. Since usually the first task to perform on an infected machine is to disconnect it from the network you can train non-information systems staff to perform this function for use in the event of a major outbreak.

Once the incident trigger has been defined and the team members are in place you can develop specific operating procedures as needed.

## CONCLUSION

Computer viruses easily pose the most common threat to your medium-sized organization's information systems infrastructure; while some are benign, others can disable or even destroy computers and the files they hold. Co-opting users into becoming part of the anti-virus solution through policy and training reduces the threat. Effective, up-to-date anti-virus software eliminates most of the viruses that remain. However, only a system that combines policy, training, software and pre-planned incident response truly offers the highest

level of protection to your organization's information assets.

## REFERENCES


[1] "Computer Virus Attacks Have Cost Businesses $7.6 Billion In 1999". Computer Economics, Inc. June 18, 1999.
URL: http://www.info-sec.com/viruses/99/viruses_062299a_j.shtml

[2] Scalet, Sarah D. "Outbreak". CIO Magazine. June 1, 2001.
URL: http://www.cio.com/archive/060101/outbreak.html

[3] Liston, Tom. "Oops, I did it again… VBS, Social Engineering, and the Homepage Worm". SANS Institute. May 16, 2001.
URL: http://www.sans.org/infosecFAQ/malicious/again.htm

[4] "Virus Primer". Trend Micro.
URL: http://www.antivirus.com/vinfo/vprimer.htm

[5] "Virus Detection and Prevention Tips". McAffee.com Corporation.
URL: http://dispatch.mcafee.com/virus_tips.asp?cid=1593

[6] "Virus Info Feed". Trend Micro.
URL: http://www.antivirus.com/syndication/vinfo/

[7] "Vulnerabilities, Incidents & Fixes". CERT Coordination Center.
URL: http://www.cert.org/nav/index_red.html

[8] "BugTraq and SecurityFocus Mailing Lists". SecurityFocus.com
URL: http://www.securityfocus.com

[9] "Microsoft Security ". Microsoft Corporation.
URL: http://www.microsoft.com/security/

[10] "SonicWall Anti-Virus Center". SonicWall.
URL: http://www.sonicwall.com/av-center/av-setup.html

[11] "Norton Anti-Virus Corporate Edition 7.5". Symantec Corporation.
URL: http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=23&PID=5951708

[12] "Trend Virus Control System". Trend Micro.
URL: http://www.antivirus.com/products/trend_vcs/)

[13] "Lower IT Costs Through Better Anti-Virus Management". Symantec Corporation.
URL: http://enterprisesecurity.symantec.com/PDF/navex_wp.pdf?PID=5951708

[14] "Anti-Virus Test File". EICAR, b.V.
URL: http://www.eicar.org/anti_virus_test_file.htm

[15] Smith, Danny. "Forming an Incident Response Team". The University of Queensland. 1994.
http://www.auscert.org.au/Information/Auscert_info/Papers/Forming_an_Incident_Response_Team.html

[16] Crabb-Guel, Michele. "NAS Security Incident Handling Procedure". SANS Institute.
URL: http://www.sans.org/newlook/resources/policies/item7.pdf

Last Updated: May 28th, 2017

# Upcoming Training


| | | | |
|---|---|---|---|
| SANS Stockholm 2017 | Stockholm, Sweden | May 29, 2017 - Jun 03, 2017 | Live Event |
| SANS Houston 2017 | Houston, TX | Jun 05, 2017 - Jun 10, 2017 | Live Event |
| Security Operations Center Summit & Training | Washington, DC | Jun 05, 2017 - Jun 12, 2017 | Live Event |
| Community SANS Ottawa SEC401 | Ottawa, ON | Jun 05, 2017 - Jun 10, 2017 | Community SANS |
| SANS San Francisco Summer 2017 | San Francisco, CA | Jun 05, 2017 - Jun 10, 2017 | Live Event |
| SANS Charlotte 2017 | Charlotte, NC | Jun 12, 2017 - Jun 17, 2017 | Live Event |
| SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style | Denver, CO | Jun 12, 2017 - Jun 17, 2017 | vLive |
| SANS Secure Europe 2017 | Amsterdam, Netherlands | Jun 12, 2017 - Jun 20, 2017 | Live Event |
| Community SANS Portland SEC401 | Portland, OR | Jun 12, 2017 - Jun 17, 2017 | Community SANS |
| SANS Rocky Mountain 2017 | Denver, CO | Jun 12, 2017 - Jun 17, 2017 | Live Event |
| SANS Minneapolis 2017 | Minneapolis, MN | Jun 19, 2017 - Jun 24, 2017 | Live Event |
| SANS Columbia, MD 2017 | Columbia, MD | Jun 26, 2017 - Jul 01, 2017 | Live Event |
| SANS Cyber Defence Canberra 2017 | Canberra, Australia | Jun 26, 2017 - Jul 08, 2017 | Live Event |
| SANS Paris 2017 | Paris, France | Jun 26, 2017 - Jul 01, 2017 | Live Event |
| SANS London July 2017 | London, United Kingdom | Jul 03, 2017 - Jul 08, 2017 | Live Event |
| Cyber Defence Japan 2017 | Tokyo, Japan | Jul 05, 2017 - Jul 15, 2017 | Live Event |
| Community SANS Phoenix SEC401 | Phoenix, AZ | Jul 10, 2017 - Jul 15, 2017 | Community SANS |
| SANS Munich Summer 2017 | Munich, Germany | Jul 10, 2017 - Jul 15, 2017 | Live Event |
| SANS Cyber Defence Singapore 2017 | Singapore, Singapore | Jul 10, 2017 - Jul 15, 2017 | Live Event |
| Community SANS Minneapolis SEC401 | Minneapolis, MN | Jul 10, 2017 - Jul 15, 2017 | Community SANS |
| SANS Los Angeles - Long Beach 2017 | Long Beach, CA | Jul 10, 2017 - Jul 15, 2017 | Live Event |
| Mentor Session - SEC401 | Macon, GA | Jul 12, 2017 - Aug 23, 2017 | Mentor |
| Mentor Session - SEC401 | Ventura, CA | Jul 12, 2017 - Sep 13, 2017 | Mentor |
| Community SANS Atlanta SEC401 | Atlanta, GA | Jul 17, 2017 - Jul 22, 2017 | Community SANS |
| Community SANS Colorado Springs SEC401 | Colorado Springs, CO | Jul 17, 2017 - Jul 22, 2017 | Community SANS |
| SANSFIRE 2017 | Washington, DC | Jul 22, 2017 - Jul 29, 2017 | Live Event |
| Community SANS Charleston SEC401 | Charleston, SC | Jul 24, 2017 - Jul 29, 2017 | Community SANS |
| SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style | Washington, DC | Jul 24, 2017 - Jul 29, 2017 | vLive |
| Community SANS Fort Lauderdale SEC401 | Fort Lauderdale, FL | Jul 31, 2017 - Aug 05, 2017 | Community SANS |
| SANS San Antonio 2017 | San Antonio, TX | Aug 06, 2017 - Aug 11, 2017 | Live Event |
| SANS Prague 2017 | Prague, Czech Republic | Aug 07, 2017 - Aug 12, 2017 | Live Event |