Global Information Assurance Certification Paper

A Case Study: Deployment of Virus Protection In The Global Enterprise

Carl H. Alexander

September 19, 2002

SANS Security Essentials Practical Assignment V 1.4 Option # 2 (Case Study)

Summary:

As security specialists we all understand the need for standards, virus protection, and security awareness. This case study shows examples of how one company's IT team ensured virus protection across a global enterprise. By reading this material you will gain insight into some situations experienced by this global enterprise due to non-standard virus protection and a lack of centralized reporting. You may relate to the headaches and loss of reputation experienced by the IT support staff due to not having information related to virus outbreaks and standard methods that prevent spreading.

We will venture down the road to standardization on a set configuration, review some bumps/successes experienced along the way and examine how standardization transformed the IT department image from a money pit into a cost saving machine. Your about to see how one IT department went from being in the dark to being well equipped to handle one of our industries most prevalent problems, virus prevention. The practical cost efficient changes we made can be applied to almost any medium size company that experiences problems due to non-standard virus prevention and a lack of centralized reporting. As reported by Info Security News Magazine, more companies are cutting back on IT capital expenditures forcing security managers to use existing tools. [1]

Before Snapshot:

The company covered in this paper is a medium to large sized global enterprise with facilities throughout North and South America, Europe, Australia, and Asia. These locations meet the strategic supply chain management needs for their customers in the healthcare, automotive, technology, and apparel industries. In each industry certain factors drive the different business models, but all rely upon effective IT systems.

The IT environment is comprised of a fairly complex network consisting of two major security sectors, the intranet network and the extranet segments. The Intranet is fairly straightforward with global connectivity from company owned sites to application hosts housed in two data centers located in the US. The Extranet is situated outside a grouping of firewalls and is composed of customer connections and connectivity needs of companies we have acquired over the past several years whose IT standards do not currently meet companies internal standards.

The IT staff has a standard 7x24 centralized support center for trouble calls, then regional field engineers are positioned at larger sites for on-site support. They travel to smaller or remote locations as required to provide on-site support in the event of major outages. The group has centralized specialist for host and network, design, installation and support located in the central office with the call center. The entire centralized staff is armed with strong authentication for remote connectivity.

From the hardware perspective the team supports some 500+ hosts that range from IBM AS400s, HP UNIX boxes to Intel based units running NT/WIN2K operating systems in the data centers. In the field locations operating systems range from Windows 98 through 2000 on normal desktops, to proprietary operating systems on handheld units used for barcode scanning across an RF Network. Most large sites have NT based file servers.

Now that you have a general picture of the environment lets look at a situation that occurred which cost the company thousands of dollars. One spring morning a support call came into the centralized support center reporting some of the RF data collectors (handheld units) at a remote distribution site for 20 customers were not functioning. The support center contacted the regional support team to investigate the outage, after 90 minutes of downtime the regional team determined the problem to be network related and called in the network administrator specializing in RF systems.

The network administrator reviewed the RF Access Points and found they were not responding to pinging or telnet related connectivity. Because normal IP connectivity failed access had to be established via a direct cable and the access points are mounted around 25 feet in the ceiling of the warehouse facility. After resetting the RF Access Point the network administrator could connect to the AP for about five minutes before it would stop responding again. After placing a network sniffer on the hardwired LAN, the network analyst determined the AP was being flooded by port "80" traffic. The traffic was coming from a host NT server 600 miles away across the Wide Area Network. This host was flooding port 80 of the RF Access points with requests it could not process thus causing the RF network to appear defective. The port "80" access point configuration method was turned off and the RF system began to function normally again.

The network analyst then contacted the NT host administrator and it was determined the host was infected with the Code Red virus which flooded port 80. Every device with an open port 80 interface was at risk of being attacked with a "Denial of Service" attack. The IT team was called to arms and spent days updating and ensuring the virus protection on 6500+ devices was working properly to prevent further service interruptions.

So after hours of patching systems, working to correct the situation the IT team had sealed the last hole which would allow such a demonic entity to corrupt their peaceful world. They report all is well, we think, but how could they be sure. Could they in truth identify how the virus got in? Could they pinpoint the time of infection? Could they prevent such a terrible thing from happening again?

Welcome to the real world of simple yet costly virus attacks. Virus attacks like this disrupt more than computer operations, they wreak havoc on a companies most valuable assets their IT people. Needless to say after two days of "I don't know" and "We think" the IT staff was on pins and needles, the operations staff was looking at costly overtime and the fact remained only a small number of systems were effecting the entire global network. A simple piece of code cost our company thousands of dollars each day while

our IT professionals scratched their heads and operation executives talked about the good old days of paper and stand-alone systems that were reliable, not like today. As security experts it is our goal to make the current working environment the best, the safest, fastest, most user friendly, while still allowing the systems to work together without an outage.

The aftermath of Code Red for our company… 400 failures to provide service to customers, 200 hours of labor had been consumed on hunting down a hardware problem that did not exist. Over 500 hours of wages were used on work around procedures because the operations warehouse employees depended upon the IT systems. The most costly loss, the company lost confidence in the IT departments ability to protect them.

The fact is either your company has a solid prevention plan with action plans for those times infections occur or your entire enterprise is at the mercy of chance and circumstance. By experiencing this situation, I developed a centralized data security area and was asked to create awareness, procedures and implement the plans for centralized reporting. The plan included writing policy, creating awareness, implementation of standard procedures and enforcement of policy through centralized control.

During Snapshot: 30
My goal was to develop a standard solution that would cover the needs of all 6500+ users in a multitude of situations. It took several months to weigh all the options and to decide upon what process would be used for standard deployment and signature updates. The company already had an enterprise level license with Network Associates to use McAfee's Virus Scan, VShield, and NetShield products. Some question we reviewed from the Information Security Handbook included: Will the vendor support this product in our environment and for how long? Does this product support inter-enterprise interaction? Does this product require deployment all at once or can it be phased in? [2]

Initial Meetings:
I initiated meetings with the regional support team management, centralized network specialists, operations management teams, and host administrators on a regular weekly basis. Concerns we covered included: What process needs to be used to deliver updates? How do we ensure each user has the same configuration? How do we report incidents to a centralized system? How will take on what roles and responsibilities.

Virus Signature Detection Update Plans/ Normal and Emergency Modes:
The plan was all workstations would be forced to check for updated at a scheduled time each day and upon reboot. The scheduled time upgrade covered those units that are never turned off and the reboot method covered those units that are not on at the scheduled update time. To avoid extra network traffic McAfee's update/upgrade program checks the source files at the update server to see if a newer version exists prior to pulling new files, this saves bandwidth when units are up-to-date and need not pull the existing files.

Having reboot trigger updates also met the need for quick response updates in an emergency type situation. Sometimes McAfee releases emergency updates for new virus

conditions that are too severe to wait for normal weekly updates. We have the ability to pull updates by just rebooting once the updates were made on the servers.

The network administrators were concerned with the amount of data 6500 users would place on the network link between the Intranet and Internet. The decision was made to have a pool of servers in the data center obtain the initial image to reduce Internet traffic. To keep WAN traffic at a minimum it was decided to have LAN servers obtain updates from the pooled servers at the data center using automated scripts that check for the latest update version. The network team agreed to monitor network traffic to ensure the updates did not overwhelm the bandwidth capacity at the data centers or at the site edge routers.

Centralized Messaging Plans:
Another concept was to ensure all virus alerts were sent to a centralized system for reporting, analyzed and follow up where required. By having a centralized repository for these alerts I could identify trends and act on conditions, as they are made known. I filtered the virus alert messages in to four categories based on the message content:
Unable to Clean/Delete, These alerts require technical intervention to resolve a situation.
Successfully Cleaned, These alerts indicated a virus was present but had been removed.
Successfully Deleted, These alerts indicated a virus-infected file had been deleted.
Blocked Files, These alerts indicate the email system blocked a possible virus file.

Departmental Assignments:
Regional supports role: The support team volunteered to cover the deployment of the standard configuration once it was established. They also developed a strategic group for beta testing the application configuration to ensure its functionality. Since this group is responsible to the internal customers directly this ensured the plan would be sold to the operations from their closest IT connections.

The NT administration team was tasked with the ability to ensure the updates were spread from the central data center servers to the remote regional servers located all across the globe. Then workstation updates could take place from the LAN and would not require the updated data files to travel across the WAN or the extranet connection more than once. Another aspect of the NT administrations task was to make the LAN look the same to traveling users so they would pull updates from the network they were on at that point in time. It was decided to use DHCP to push out a local domain entry that would have an entry for the local update server. The local domain allowed the data security group to name one source in the standard configuration, and the local domain would direct the users update to pull from that local domain's update server.

I was tasked to develop the standard configuration to meet the needs across a variation of Windows operating systems. Using McAfee 4.5.1 we ran test after test after test until we found a solid beta configuration we knew would meet the needs of the support team. During the same time period we worked with the regional support team to develop a planned deployment strategy that would meet our companies needs. We also coordinated tests with the NT administrators to test the update scripts and the reliability of the local

domain concept. Documentation for the standard setup of McAfee defined how the application was configured. A policy was developed to define the use of McAfee and how to report incidents. The documentation was used to help in the testing phase.

Test Period /Verification Team:
Over a fourteen-week period we ran through beta tests with a group called the verification team. The verification team was made up of regional support technicians, support center staff, NT administrators and network administrators. During the test phase the standard configuration image had to be tweaked several times to accommodate the needs of the technical support staff as well as the NT administrators.

The original configuration had one data security password to lock the entire configuration, however this did not allow the field support team to make needed changes to the scheduled time of the update to prevent downtime in the operational areas. To resolve this concern I added a second password for the update time and share it with only the technical support personal. The original password still controlled the upgrade path and scanning configurations so that only a couple management team members and myself had the ability to change these settings.

The second adjustment to the configuration came due to a naming convention change forced by the NT group to enable certain DHCP aspects of the local domain configuration. This change involved the path of the update/upgrade server that is to be used by all workstations whether desktop or mobile laptops. DNS at the local level will define the closest update server so all users can use the same McAfee image file to receive updates without having to reach across the WAN for updates. This allows all workstations to update from the LAN level and only servers in each region will update from the central pool located in the data centers.

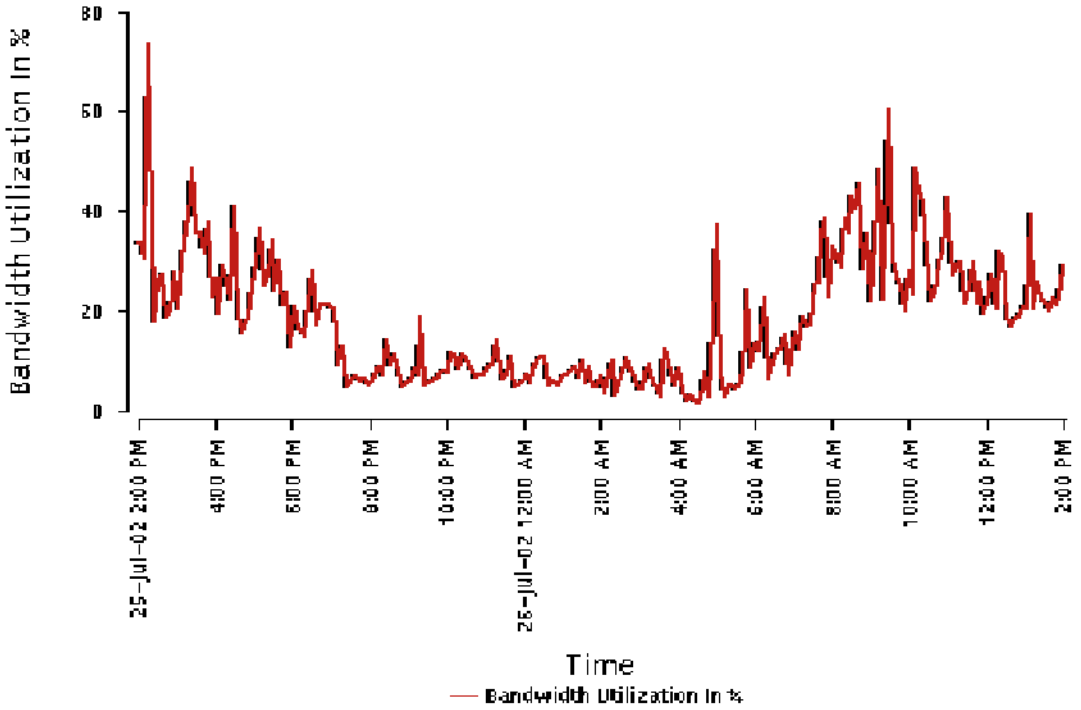
Because of the automation aspect of these updates the question was raised, what happens if an update pulled by the central server pool is corrupted? All 6500 devices would be updated by a corrupted file that could cause downtime. The solution was to have the verification team continue meeting on a weekly basis to verify the update files prior to moving them to the centralized server pool. To test the updates the verification team would verify the files against a grouping of test systems pulling up updates from a staging directory on the update server pool. Once confirmed clean the update file would be moved to production and then automatically be pulled by regional servers. To acknowledge the update files were validated the verification team sends out an alert to all technical stakeholders indicating the new change and version verification.

At the end of the test phase I used McAfee Installation Designer version 1.1 to create the final McAfee Setup file for installation for the all systems. The final configuration installation was used to create a disk image for new implementations to make sure the procedures and setup were identical for future systems as well as current installations.

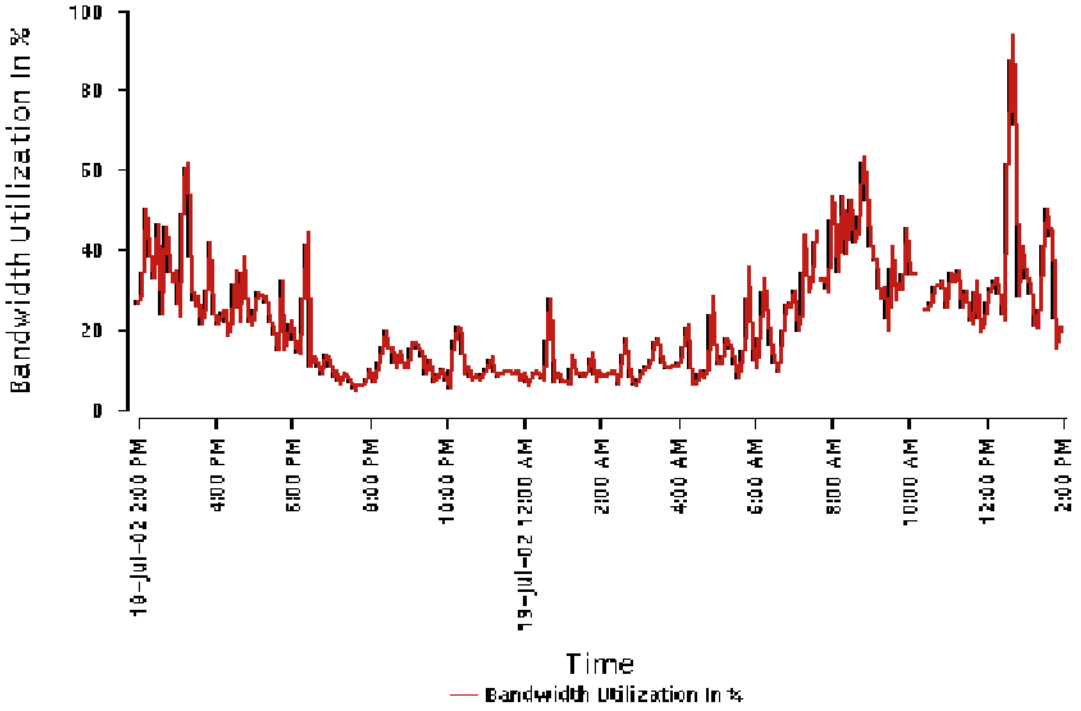
Deployment Plans:
As mentioned before I had been working with the regional support management team to develop the plan for deployment. We had 7 regional management teams to work with, 4 in the Americas, 1 each in Singapore, Europe, and Australia. We planned the initial deployment in the Eastern Region of the US. We needed a strong on-site support presents for this first phase of implementation to make sure the project was successful.
Awareness for IT and Operations:
The first step in the deployment plan was to announce the planned changes on the weekly technical change control call that had an international audience across all business units. The initial reaction from the announcement was calm because I had already made contact with the business analysts in each area to explain the changes we were making and to ensure all questions had been answer prior to this critical point. Our company uses the change control format to ensure all parties are aware of technical changes that may affect their areas of operations.

Initial Site:
A waiting period of two weeks pasted, then the first DNS changes were made and the DHCP server scopes were checked for compliance. By pinging the name of the DNS entry for the update server from a unit on an updated VLAN we knew whether the DNS changes were working. The ping responded with the local servers name and we were ready to install the image on the first 50 of 1200 workstations. After the initial installation one unit was called in as not updating, it was discovered this unit had not been properly configured for DHCP to accept the Local DNS entry, after this was fixed it worked properly. After fourteen days of operations the 50 units had pulled two weekly updates properly and the scanning and alert systems were working properly. The network team continued to monitor the edge router traffic to make sure the systems were pulling updates from the local server and not across the WAN. Here are graphics to show the WAN traffic was not being affected by the updates.

Circuit Utilization 7/25 - 7/26 **LTLC** INBOUND TRAFFIC



Circuit Utilization 7/18 - 7/19 **LTLC** INBOUND TRAFFIC



The green light was given to start the other 1150 units and the NT administrator worked with the network administrators to identify the VLAN segments the DHCP scopes would affect with the DNS changes. We only changed the DHCP scopes as the regional support teams were ready to install the McAfee image. By waiting until the support staff was

working on a segment we avoided any possible problems not being addressed during the changes to DHCP.

The other aspect of the local DNS changes was the stations with static IP addresses would need to be configured for the new local DNS information manually. We did discuss the possibility to see if a script could be written to address these stations but decided the effort would not be worth the time considering the number of static IP addresses we had to deal with.

Message Server:
At this point the message server started receiving alerts from the first site as virus signatures were detected, most came back as successfully cleaned, but several units were infected with the Nimda virus. Trouble tickets were opened on these units and the support staff cleaned these with Nimda removal tools. We had been infected all along, we just did not know it because the virus was not causing major problems on these units and the users were not reporting the alerts. This discovery did not surprise us it just enforced our need for centralized reporting so we could determine the true state of our network. By the end of the initial installation we received over forty thousand alert messages indicating mostly cleaned Nimda infections, but about 40 units had to be manually cleaned.

Continued Deployment:
With the success of the initial site rollout the deployment to all other regions was given the go-ahead. Most sites had similar instances where either the DHCP entry for the local DNS failed due to configuration error units or the need to address static IP address configurations. One site did have a special need we had not foreseen, the normal language used for our deployments had been English, however our Asia sites were already using Japanese, Korean, Chinese Traditional (Big 5) and Chinese Simplified (GB). McAfee offered a solution called McAfee Double Byte that uses Unicode characters to translate the needs of these languages. Through our license agreement with McAfee we were able to obtain this application at no additional charge and it worked perfectly for our needs.

Awareness:
Each week during the deployment the company received executive summaries detailing the progress of the rollout team as well as the latest statistics on alert messages. This helped to improve the image of the IT team as the findings indicated we were being proactive in addressing possible future issues. Based on the number of automated cleanings reported we were able to indicate the effectiveness of the virus prevention software. Most possible virus infections files were caught by the VShield application that does not even allow the virus to infect a unit in the first place.

Each week I would also send an update indicating what new virus signatures were to be addressed by the newest update files to all verification teams and regional support teams so they could share the information with their areas of support. This raised the level of awareness within the IT department which then flowed into the operational area. In

addition to the virus updates I included the most recent statistics from central reporting information I was analyzing, specific items like the most virus causing the most Alerts or the newest virus our systems have cleaned.

After Snapshot:
Now on an hourly basis an automated FTP process checks the Web for new virus signature data files and pulls them to a staging directory on a Unix host system. A group of 30 verification team members have workstations that are automatically updated from the staging location and verified the file during either a weekly call or an emergency update call. This team is responsible for the integrity of the update files and for making them available to the centralized production server pool consisting of 3 NT servers located in our data centers which are accessible by only servers on our network.

The NT administration team has configured the regional servers to check the data center servers for updates on an hourly basis. When updates exist, the servers automatically pull the update files and start the automated scanning process. If virus signatures are found messages are sent to a centralized message server and these are reviewed by data security. If automated cleaning cannot address the situation a trouble ticket is opened at the customer support center and the NT administrators are dispatched to address the concern. Once addressed, the ticket is closed and the data security team is informed of the status of the ticket.

From the regional support level the local workstations or traveling users using DHCP either pull updates at a scheduled time during non-operational hours or upon reboot of the workstation. If no new virus prevention files exist the process is repeated at either the scheduled time or at the next reboot. The scanning process on all workstations is set for a strategic time just after the weekly update is made available to the workstations. This is just prior to the weekend, which provides the IT support staff with time if a serious virus infection is discovered by a new set of virus detection files. All 6000 user stations report alert information directly to the centralized message server for analysis. The data security team reviews the messages and follows the steps as described above for server infections.

A centralized message server is setup to prioritize the messages received from the 6500+ devices on the enterprise network. These messages indicate the status of a particular workstations condition. The messages are formatted as such:
The file C:\TEMP\mepCD7.tmp.exe was infected with W32/Nimda.gen@MM Known Virus, Detected with Scan Engine 4.1.60 DAT version 4.0.4213. The file was successfully deleted.(from LT1ARM114EL19 IP XXX.XXX.43.194 user GENERIC-MASTER\jebennett running VirusScan 4.5.1 OAS)

From the information contained in the message above we can identify the workstation name, the IP address being used, the users ID, the file that is infected and the virus infecting the file. We can reference McAfee's web based virus information on this particular virus at http://vil.nai.com/vil/content/v_99209.htm [3] More importantly were can see the condition of the workstation and decide what action needs t be taken to address the situation. By utilizing the user name and our Outlook global address book I can

directly call the user and let them know to take action if needed to prevent further infection or to advise them of possible problems they may see. In any case data security now has the ability to know what is happening.

In addition to the alerts from server and workstations our email system uses McAfee to block certain file extensions know to contain possible virus infections. As these are not always virus related alerts they are less likely to require immediate attention. Our company has a very strict policy on the use of Email and all email users sign documentation indicating they agree to follow our email policies. Because of this I review these alerts and have found several virus situations in the initial stages before they have a chance to mass-email the entire company. The alert message is similar to the one above but indicates a file has been blocked. I normally send a nice message from the data security department to raise the awareness of the individual using our system. This is and example of a message I sent recently to a user who had a friend transfers game files:

Good Morning,
This is an alert from the Data Security team to let you know your email accounts and workstations should be audited based on emails sent to you that had blocked content. Due to the nature of Virus Signatures your units may be infected thus causing additional damage to the company network. Please work with your management team to have your workstations proper reviewed for virus infections. The alerts below indicate an outside email account sent several emails with attachments to you, the outside account is listed as Melissa (Melissa@xxx.xxx) Please understand your compliance to all Email guidelines will help prevent virus infections. Thanks, Data Security

Impact:

Confidence in Systems:

Now that our company has deployed a standard virus prevention program with a locked set of configurations we have been able to reap the benefits of our efforts. Based on my analysis of the centralized alert information I can safely state our network is running clean at this point in time. I have the ability to state that over 6500 devices I monitor are currently not sending messages indicating virus infections. I can report to our sales team that we have another layer of security they can sell to our customers. In an article called "The Computer Virus of the Future" the author notes viruses will become more sophisticated and those who are prepared will win the war in the end. [4]

Work Place Attitude:

Now that we have a policy, a procedure and proven methods for the prevention of virus infections in place the IT team has the time to relax, yeah right, but we don't worry about virus infections as much as before and neither do our operation mangers or company executives. They have seen the effects of our efforts and have awarded our staff with tokens of recognition.

No Service Failure Type Outages:

Since our company implemented the above processes we have not been caught in a situation were production time was lost due to an infected workstations or server. We

have been infected and have been able to locate and control the infected stations. The bottom line is because we invested the time to devise and develop a strategy to prevent virus infections at the enterprise level we are now more effective and save money.

Ability To Address Infections:
If a virus happens to make it through the prevention phase due to late updates or individuals not following company policy I am the first to know when an alert is issued. I have opened trouble tickets and called users directly. I let them know the data security team is on the ball and protecting our company's interests. Based on the past few months we can show where the automated systems have cleaned over 30 thousand infected files automatically. I also have records indicating the situations where data security got involved to prevent the spread of know infections. We now have the ability to update the virus prevention files for the entire company's inventory of servers, workstations and mobile users in a minimum of 24 hours and as little as 3 hours if required. An article about McAfee mentioned the upcoming ability to manage other AV systems in the near future. Those enterprises that do not have one AV system will find themselves wanting.[5]

Customer Assurance:
Another advantage to our virus prevention efforts is our ability to let our customers know we are active in the prevention of virus signatures. Dealing with us they can be assured we are taking every reasonable measure to keep our systems running and protecting their interests. When another companies data security team hears we have centralized alert systems and 24x7 coverage, we have the ability to back it up in writing and making sure our internal and external customers are confident in our systems is the true goal of IT.

References:

[1] SC Info Security News Magazine, April 2002 issue
Pg. 27, Cheap Tricks for Information Security – Author Chris Cunningham

[2] Information Security Management Volume 3, Handbook Edition #4
Chapter 24, Pg. 447-8, Information Security in the Enterprise – Author Duane E Sharp
Copyright 2002

[3] McAfee's Virus Signature Database (NIMDA Virus Profile)
http://vil.nai.com/vil/content/v_99209.htm

[4] News Factor Network (NewsFactor.com)
"The Computer Virus of the Future" Author Lisa Gill (March 3, 2002)
http://www.newsfactor.com/per1/story/17590.html

[5] Future Com (MyFutureCom.com)
"McAfee Manages Symantec With ePolicy Orchestrator" PRNewswire(Oct 29)
http://www.myfuturecom.com/veiwnews.asp?id=1015