Implementing an Antivirus system as part of an overall ISO 17799 ISMS

Dave Shackleford

G17799 certification, version 1.0

April 25, 2004

I. Define The System

The company is in the field of transportation and travel services; specifically, a low-fare airline operating in the continental United States (primarily in the Eastern half of the country). The company has been in business for approximately 10 years, with varying management and names, but is doing extraordinarily well under the current management. Thus, the company is expanding rapidly to Western destinations, and currently serves 46 different cities, with plans to go to as many as 70 in the next 2 years.

The company's Information Systems department has never had a Security Manager, and any technologies implemented have been sparsely managed by the Systems Administration or Network Administration teams. As the new Security Manager, I am tasked with creating policies, implementing technologies to mitigate risk, and analysing the processes and systems in place to make them more secure. The company has approximately 2000 regular computer users, spread out in all 46 different locations that the planes travel. Locations in Orlando, Florida; Savannah, Georgia; and Atlanta, Georgia (especially) have large concentrations of users. The company headquarters is in Orlando, while the IT department is entirely based out of Atlanta. Other than 8 full-time staff members onsite in Orlando, the entire IT staff is based out of Atlanta, the company's primary hub of operations (Atlanta's Hartsfield-Jackson International Airport).

The CIO has mandated that an ISMS be developed, using the ISO17799 methodology. As the scope of the organization's information assets is large, he has requested a precursory risk assessment within the organization to determine what systems need primary attention in being constructed and implemented. Based on an assessment performed by an external auditor, several major areas needing improvement were identified. These auditors followed the Risk Assessment strategy espoused by NIST, which uses a matrix as follows (7):

Threat likelihood	**IMPACT**		
	LOW (10)	**MEDIUM (50)**	**HIGH (100)**
HIGH (1.0)	Low (10x1.0=10)	Medium (50x1.0=50)	High (100x1.0=100)
MEDIUM (0.5)	Low (10x0.5=5)	Medium (50x0.5=25)	Medium (100x0.5=50)
LOW (0.1)	Low (10x0.1=1)	Low (50x0.1=5)	Low (100x0.1=10)

Risk Scale: High (>50 to 100); Medium (>10 to 50); Low (1 to 10)

The following were identified as the top 2 threats:

- Viruses and malicious code inside the network – 100
- Business Continuity Planning, Disaster Recovery – 50

Based on the threat likelihood (very high), and the potential impact (also very high), the first and foremost of these potential risks (with a score of 100) is the presence of huge quantities of viruses within the corporate network. Also, there is no centralized management system or procedures for installing and maintaining client software to prevent and detect malicious code in place. Several major factors tie into this, as well:

- The company's network architecture is constructed such that all traffic passes through the data center (hub) in Atlanta. Thus, effective bandwidth management is integral. Viruses can rapidly consume large amounts of bandwidth, especially in remote locations such as airport stations where lower total bandwidth is available.
- The means for dispatching Field Services staff to the more remote locations to fix viruses or re-install software and/or operating systems is hindered by the fact that the company is so distributed, and the Field Services staff operate out of Atlanta.
- The company's email system is now relied upon as a major business tool, tied directly to revenue stream, customer service quality, and internal communications.

Bases on this assessment, the primary issue now concerning the CIO is the development of a distributed and manageable antivirus system for servers, workstations, and email filtering. All three exist to some extent, but no updating has been done in some time, no centralized management has taken place, and no policies exist to govern the correct or expected use and implementation of this type of application. The company has been inundated with viruses over the last 2 years, and no one has been able to centrally coordinate a means of controlling the problem. Using an ISO17799 methodology, I intend to develop and coordinate a system consisting of a comprehensive antivirus management solution, using some existing resources and implementing some new products and techniques as well. I will evaluate the system's success using the rate of virus infections and other metrics in a before and after fashion. Some of this work has already been done, and some remains to be completed.

Briefly, the system that exists currently is one Norton Antivirus Server, managing approximately 1200 Norton Enterprise 7.5 and Symantec Client Security 8.0 clients. No central console is managed by anyone. The clients consist of 300 in Atlanta, 300 in Savannah at a Reservations Center, and 300 more in Orlando. The remaining 300 clients are located in the various airport stations where the company operates. The server-level antivirus consists of McAfee NetShield 4.5, sparsely installed and managed on 75 servers located in Atlanta and 15 more in Orlando. The corporate email server is running Trend Micro ScanMail 6. The internal LAN in Atlanta is Gigabit Ethernet mixed with 100BaseT Ethernet. The Orlando Headquarters location is using 100BaseT, and the connection between them is a fairly fast Frame Relay circuit. All of the airport stations are connected with varying speed connections (256K up to T-1).

To include some more background information regarding the organization, the culture of the organization has been one of very rapid growth. The IT management has been fighting to keep up with demand, and very little thought has been given to overall security of the IT infrastructure. With a very "costconscious" culture, the company tries to make the best use of its existing resources and spend more money on IT only when necessary. Thus, to date, what security has been in place has largely been managed by the Network team and the Systems Administration team.

The company's security program is in its infancy. No policies exist yet, and no corporate security awareness program has been created. No real processes exist to manage the antivirus system that is in place. Very few controls are in place. When the systems administration team has time, they check to make sure the client definition file updates are pushed out to Desktop clients, and the server-level antivirus software is never checked. No alerts are sent to anyone when a virus is detected. If a user calls the Help Desk, the ticket is assigned to a member of the Field Services team to look into the problem. No program is in place for the Field Service technicians to receive the most up-to-date tools and instructions for virus removal and machine restoration.

This paper will serve to accomplish several major components of a total ISO 17799 security program, all related to the antivirus system:

- First, as the virus problems are a major impetus to the senior management hiring a Security Manager and backing a corporate information security program, a committee will be formed to discuss the controls and systems in place and the ones needing consensus for creation.
- The existing controls will be upgraded to be more effective and efficient.
- A corporate antivirus policy will be written and approved by senior management.
- A corporate information security awareness program will be created. As this entire project would be beyond the scope of this paper, only the antivirus portion will be featured.
- The overall antivirus system in place will be refined and, with documentation, will become a complete system operating within the framework of a larger ISO 17799 ISMS.

II. Plan

The first step in this phase is to accurately define the real problems at hand. These are portrayed as risks that are mapped directly to business objectives.

Business Objective	Provide fast and reliable customer service to customers at stations and reservation centers during all business hours.
Risk	Customer service agents use PC-based systems that run software for booking flights, accepting customer payments, etc. If virus infection compromises the speed or integrity of the operating system on these systems, agents may be unable to provide customers with relevant information or services.
Control	Centrally monitored desktop antivirus software running at all times as part of a comprehensive antivirus system within the framework of the corporate ISMS.

Business Objective	To reduce corporate telephony costs by implementing a corporation-wide Voice over IP (VoIP) system that is use for both office telephones and standard ‘terminal’-type phones, as well as PC-integrated headsets for customer-service reservations agents.
Risk	A successful VoIP implementation relies on effective bandwidth management and QoS design. Viruses within the corporate network may create broadcast or other traffic that consumes valuable bandwidth, degrading the quality of the corporate telephone service or disabling it altogether in lower-bandwidth areas.
Control	A comprehensive antivirus system, particularly desktop-level and server-level antivirus software that effectively updates virus definitions and provides preventive and detection controls for malicious code.

Business Objective	Improve on-time performance of all aircraft by effectively communicating with aircraft and all ground controls with regard to scheduling, departures and arrivals, maintenance, etc.
Risk	Real-time communications are essential to meeting on-time performance goals for all aircraft. Various mission-critical systems play an integral part in this; these are used 24 hours a day and 7 days a week by numerous groups within the organization, who must access various files and other programs from servers. Corrupted files from virus activity could severely impact the ability of these groups to perform their duties in a timely manner.
Control	Server-level antivirus software that is continually updated with the latest virus definitions, as part of a comprehensive antivirus system within the framework of the corporate ISMS.

Altogether, the scope of corporate information assets that must be protected from malicious code is quite substantive. All workstations related to customer service, such as those in the airports and reservations centers, are directly related to the primary revenue stream for the company. Thus, the threat of malicious code to end-user workstations is palpable, as customer service quality is a major business driver in the transportation industry. The number of mission-critical server systems that support air-traffic control communications, calculations for aircraft weight distribution, fueling capacity, maintenance records, etc. is also of foremost importance, and is monitored by government entities such as the Federal Aviation Administration (FAA). Thus, the risk to these systems from malicious code could also pose massive harm to the company. Finally, as email is a particularly viable threat vector for viruses and other malicious code, antivirus software running on the email gateway is also considered vital to the success of the antivirus system.

Now that exact risks have been identified, defining the actual problems from a baseline perspective is important. Without effective centralized consoles for management of antivirus clients, or any logging or monitoring capabilities in place, some estimates have been made in terms of the current virus infection rates and issues within the organization:

- Based on the volume of Help Desk calls related to virus activity, desktop-level virus infections and attacks are being experienced on roughly 25-30% of the corporate end-user workstations on a monthly basis. This comes to approximately 300-400 clients infected with viruses at any given time.
- There are an estimated 300-500 workstations with virus software installed that is out of date with the corporate standard, and is not being monitored by a central Symantec server. There are also anywhere between 50-100 new workstations being added each month that need to be managed, as well.
- A final problem related to the desktop antivirus software, in particular, is the ability to alert the security staff, Help Desk, and Field Service when infections are detected.
- The server-level antivirus product, McAfee NetShield, is not supported actively at this time, and upgrades are needed. Based on the limited reporting capabilities in the product, it has been determined that servers in the company are experiencing virus infections or attempted infections at a rate of 10-12 per hour. The performance hit from this program running is also significant.
- The email gateway antivirus software, Trend Micro ScanMail 6, needs some adjustments. No one has properly configured attachment blocking or automatic updating. Currently, viruses are being detected coming in at a rate of 5-10 per hour. It is suspected, however, that due to improper configuration, the outbound virus traffic (via attachments, typically) is fairly significant. An estimate might be 10-20 per hour.

The Security Committee decided that the following metrics would be used to determine an overall level of success with the antivirus system being designed:

- At the desktop level, a decrease in virus infections of 90% was chosen as a target. This would translate, based on estimates, to no more than 40-50 infected clients at any given time within the enterprise. This will be easily monitored using the Symantec System Center Console.
- A more distributed architecture is established to manage the desktop clients and provide automated updates and virus definitions. We would like to see, based on future audits, less than 2% non-compliance in terms of managed software with the established corporate configuration. This would translate, roughly, to 10-20 machines at the most without a managed and completely automated installation of Symantec Client Security.
- A sound system is in place to monitor server-level antivirus logs on a daily basis.
- The server-level antivirus software is updated, and the rate of virus infection/attempted infection is reduced by 90% or more. This would translate to no more than 1-2 per hour at the most, per server.
- Email antivirus software is blocking attachments with all extensions other than ZIP, which is deemed necessary for business purposes. Both outbound and inbound virus scanning is effectively blocking all viral content at all times. Automated signature updates are enabled, refreshing every hour. Although it is not possible to alter the flow of incoming virus attempts, the rate of outbound blocked attachments and viruses should decrease significantly (90-95%), to no more than 1 per hour.

The implementation of the improved antivirus system will require intense planning and cooperation for the actual implementation. The timeline for the project has been set at 6 months, with a relatively simple project plan to start (3):

Month 1:

- Assess the existing assets in the organization that act as components of the antivirus system.
- Create a baseline for the existing problem, to measure against in the future (relates to above estimates).
- Create a team to implement and plan the system.

Months 2-3:

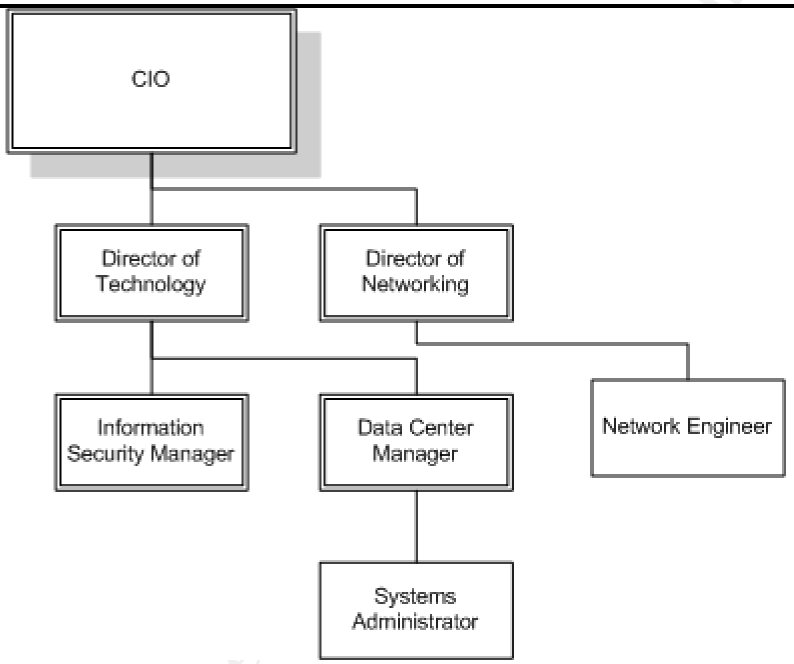
- Develop policies and procedures that will encompass the updated antivirus system.
- Determine what controls exist, and which are needed.
- Choose products to upgrade the system.

Months 4-6:

- Implement and test the new products.
- Create a security awareness program component related to the antivirus system.

- Hand off administrative duties involving the antivirus system to the Help Desk and Field Services staff, with training on all new policies, procedures, and technologies.
- Document the new state of the system, with metrics to demonstrate improvement (based on above estimates).

The management structure of the IS department is very straightforward. The involved parties are shown in the following hierarchical diagram:



Organization's IS Department Structure

Any capital expenditures will need to be approved by both the Director of Technology and CIO, but both have given the full direction of the project to the Information Security Manager. As a dedicated security position is new to the company, the management is more than willing to let the security manager take over roles and responsibilities that had previously been underrepresented by the other groups. For example, network intrusion detection had been managed by the Director of Networking, as had overall access control design. The Data Center Manager had been delegating basic implementation of antivirus management to her staff of administrators. In addition to the hierarchy above, a Help Desk team and Field Services team both report to the Director of Technology, with a Supervisor over each team that must work for and with the Information Security Manager and Data Center Manager.

No company information security policies exist at the moment. With relation to the antivirus system, a total corporate antivirus policy will have to be defined and written. Standards for products to be installed, as well as procedures for the installation, will have to be documented as well. Finally, guidelines for virus detection and “common-sense security” related to viruses and antivirus software will be outlined as part of the corporate security awareness program.

As the IS team is small (around 55 people), the number of people available to assist with the project is small, as well. The primary responsibilities will fall on the Security Manager, with assistance from one Systems Administrator and one Network Engineer. The other management will also be involved to varying degrees. This group will identify all server-level assets pertaining to the antivirus system. The Field Services team is responsible for configuration of all user desktop machines, and so the workstation assets are documented by them.

The Security Manager will identify and asses any risks to the information infrastructure, and develop a simple plan for risk management by increasing controls and implementing them effectively, upgrading software to newer versions, setting up an alert system for incident response, and training the staff to centrally manage the updated systems.

The company will create a brand new Information Security Committee to address not only the antivirus system being implemented, but all other policies and procedures (including technology-specific information) as well. The Committee will consist of the following individuals:

- The CIO
- The Director of Technology
- The Director of Networking
- The Data Center Manager
- The Information Security Manager (me)
- 2 Field Services Supervisors
- The Help Desk Supervisor

This group will act as the steering Committee for all security initiatives. The following individuals/teams will be most applicable for the antivirus system, as well as the later systems to be implemented under the ISO17799 ISMS:

- Information Security Manager – Manages the project, process, and technology choices from a risk analysis perspective. This will involve taking stock of the existing rate and number of virus infections, examining controls, and writing policies. The security manager will also evaluate the correct implementation of the system.
- Data Center Manager and Systems Admin team – This team will be the implementers of technology related to the system. Any servers will be configured and installed, antivirus packages for desktop installation will be staged, and definition file replication methods will be installed.
- Field Services/Help Desk teams – These teams will be the monitors for any end-user implementation, incidents related to virus cleanup, etc. within the system. These teams will be alerted first when virus incidents

occur, and will be the teams that either manage the issues or escalate the problem to the security manager and others.

The CIO and Director of Technology are involved as senior management participants who will sign off on policies and procedures and approve expenditures related to the system. The Director of Networking is responsible for all use of corporate bandwidth, as well as the company’s routers, firewalls, and switches. The other participants will all be directly involved in the planning and implementation of the actual system technology and architecture.

The policies that will be created can be lumped together into one large company-wide antivirus policy. The general information within the policy will be straightforward and simple, using information taken directly from the SANS Policy Project:

> **1.0 Purpose**
> To establish requirements which must be met by all computers connected to <Company Name> networks to ensure effective virus detection and prevention.
>
> **2.0 Scope**
> This policy applies to all <Company Name> computers that are PC-based or utilize PC-file directory sharing. This includes, but is not limited to, desktop computers, laptop computers, and servers of any type
>
> **3.0 Policy**
> All <Company Name> computers must have <Company Name>'s standard, supported anti-virus software installed and scheduled to run at regular intervals. Non-server systems will use a managed client, with virus definition files installed automatically. All software will be installed by members of the IS Department.
>
> Any user detecting a virus via software alert or other virus-indicative behavior (see <Company Name>'s *Anti-Virus Recommended Processes*) must call the IS Help Desk to report it. Virus-infected computers must be removed from the network until they are verified as virus-free. The MIS Security Administration team is responsible for creating procedures that ensure anti-virus software is run at regular intervals, and computers are verified as virus-free. Any activities with the intention to create and/or distribute malicious programs into <Company Name>'s networks (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are prohibited, in accordance with the *Acceptable Use Policy*.
>
> Refer to <Company Name>'s *Anti-Virus Recommended Processes* to help prevent virus problems.
>
> **4.0 Enforcement**
> Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Revision History

This policy will touch upon the following of the 10 key ISO 17799 controls:

- **Allocation of information security responsibilities within the organization** – the policy states that members of the MIS Department will be the only ones to install and configure the software, and that the MIS Security Administration team will be responsible for setting the software to run at regular intervals, and checking PC's to make sure they are virus-free before being returned to the network.
- **Virus detection and prevention controls** – this policy specifically relates to the antivirus system within the organizational ISMS.
- **Protection of personal data** – as viruses often access documents or email on user's machines, the prevention of malicious code will deter the unwanted dissemination of personal data.

As far as risk analysis is concerned, I decided to create a process based around the method of Time Based Analysis. First, the policy objectives were defined:

- The preventive controls should prevent any malicious code from entering the organization.
- The detective controls should quickly and efficiently detect any malicious code that does happen to enter the organization.
- Reactive controls should allow the organization to quickly respond to the malicious code and recover from the threat.

Then, the following controls were defined (4):

Preventative Controls (8)

- All <Company Name> desktop or end-user computers must have <Company Name>'s standard, supported anti-virus software installed and scheduled to run at regular intervals.
- All <Company Name> servers must have <Company Name>'s standard, supported anti-virus software for servers installed and scheduled to run at regular intervals.

Detective Controls (8)

- All <Company Name> computers must have <Company Name>'s standard, supported anti-virus software installed and scheduled to run at regular intervals.
- All <Company Name> servers must have <Company Name>'s standard, supported anti-virus software for servers installed and scheduled to run at regular intervals.

- For desktop software, the central reporting server must be configured to send an email alert to the MIS Help Desk upon detection of malicious code.
- Any user detecting a virus via software alert or other virus-indicative behavior (see <Company Name>'s *Anti-Virus Recommended Processes*) must call the MIS Help Desk to report it.

Reactive Controls (8)

- All antivirus software is configured to first quarantine malicious code; if this fails, the software is configured to delete the code.
- Any user detecting a virus via software alert or other virus-indicative behavior (see <Company Name>'s *Anti-Virus Recommended Processes*) must call the MIS Help Desk to report it.
- The MIS Help Desk must be able to receive various forms of alerts sent by the central antivirus reporting servers.
- Virus-infected computers must be removed from the network until they are verified as virus-free.
- The MIS Security Administration team is responsible for creating procedures that ensure anti-virus software is run at regular intervals, and **computers are verified as virus-free**.

In the case of the antivirus system, these controls are straightforward and simple. The Preventive controls are only effective when the corporate standard antivirus software is installed and configured properly on all workstations and servers. As this software is integrated with the operating system and file structure on each machine, this will effectively combat any known malicious code defined in the software's definition files. The only weakness in these controls involves "zero-day" malicious code that may not be included in the software's definitions.

The Detective controls also require the installation and configuration of the aforementioned software. Typically, such software can respond almost instantaneously to malicious code detected on the machine, performing one of a number of possible actions; these include quarantining the file(s), deleting the file(s) altogether, or doing nothing. The workstation-level software also reports to central alerting servers, which are configured to send alerts to any number of different parties. This is a key control in enabling the Reactive controls to be effective. Users are also trained to contact the MIS Help Desk when a virus alert is activated on their local machines.

Finally, the Reactive controls collectively aim to mitigate the risks as quickly as possible. The local antivirus software is set to quarantine, then delete files that are labeled as viruses or other malicious code. The end-users of workstations are instructed to contact the Help Desk in case of a virus alert or infection; the central alerting servers are set to email the Help Desk mailbox upon detection of any infections or infection attempts, as well. The Help Desk is then to instruct users to remove their network cables when applicable, and the Security

Administration and Field Services teams are contacted to eradicate the viruses, if necessary, and verify that the machines are “clean” for reinstatement on the network.

If the preventative controls fail, what sort of detection and reaction times can we expect? The first step is to determine the worst case scenarios for detection and reaction.

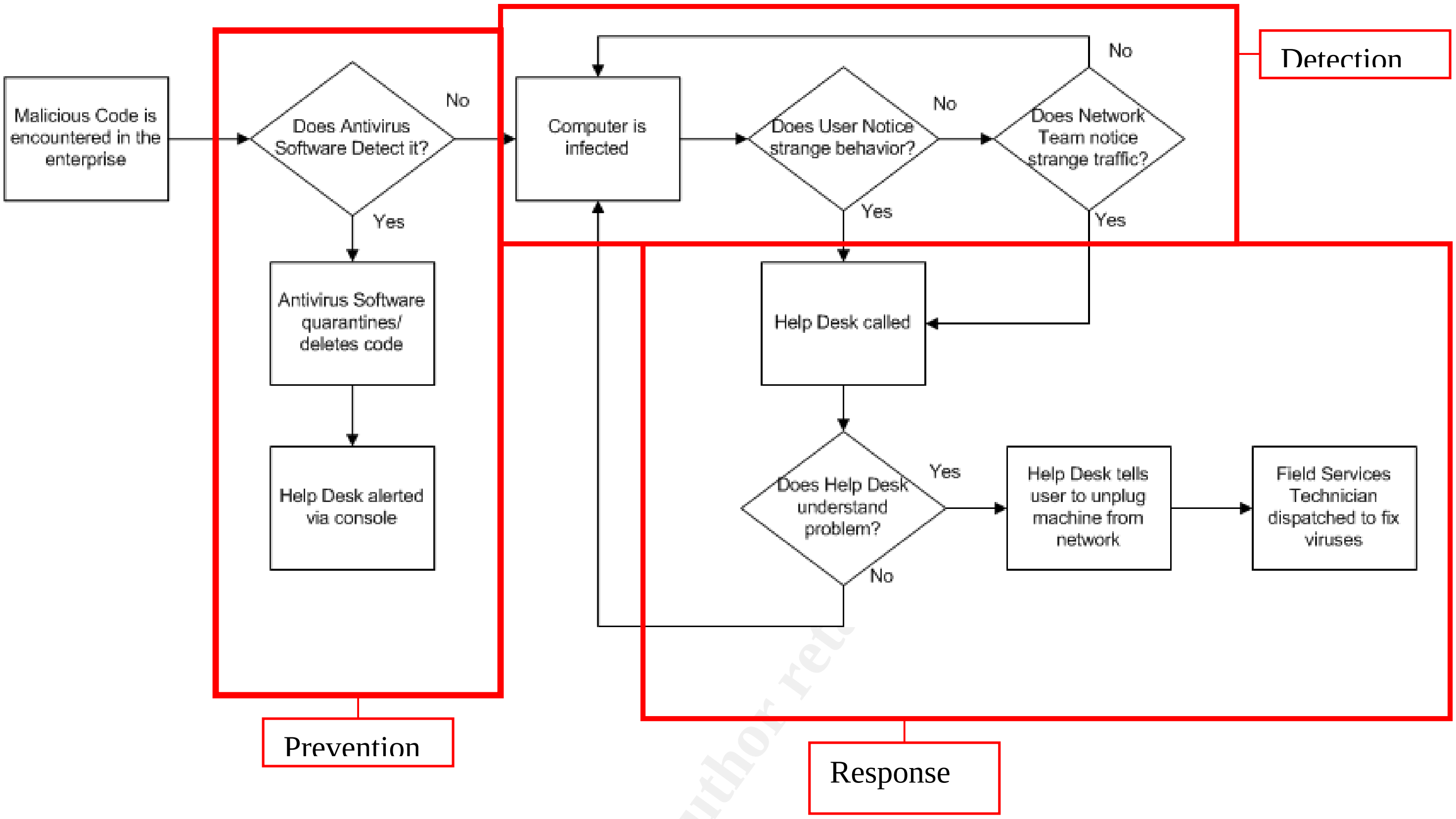
The worst case for detection was targeted at 4 days. The Director of Networking and his staff are extraordinarily vigilant in looking at anomalous or excessive network traffic. The company has recently embarked on a full-blown IP Telephony strategy, so network bandwidth utilization can dramatically impact the quality of phone service, a business-critical application. If the preventative controls failed, and virus traffic on a specific VLAN or network segment increased for any reason, the network engineers would undoubtedly notice it within several days.

The worst case for reaction and eradication was targeted at 3 days. Being an airline, many network locations are widely dispersed airports in a large geographic area. Sometimes, the Help Desk cannot effectively dispatch a Field Services technician to one of these airport locations quickly.

The following spreadsheet was derived from the course training for determining what sort of detective and reactive times we have come up with (8):

Event	Detect Time	Response Time	Exposure Time
Virus Infection Worst Case	4 days	3 days	168 hours
Virus Infection Best Case	1 second	1-2 seconds	2-3 seconds
Virus Infection Target	1 hour	3 hours	240 minutes

At this point, to determine the major risks, we created a process flow chart that would illuminate where our points of critical failure might be:


Malicious Code is encountered in the enterprise
Does Antivirus Software Detect it?
No
Yes
Antivirus Software quarantines/ deletes code
Help Desk alerted via console
Computer is infected
Does User Notice strange behavior?
No
Yes
Does Network Team notice strange traffic?
No
Yes
Help Desk called
Does Help Desk understand problem?
Yes
No
Help Desk tells user to unplug machine from network
Field Services Technician dispatched to fix viruses
Detection
Prevention
Response

Where are the major failure points? We decided that the following would be the worst points of failure:

- Antivirus protection fails completely (first line of defense).
- User and/or Help Desk does not understand problem well enough to rectify.
- Help Desk is unavailable for an extended period of time, possibly allowing virus to propagate.
- Field Services team does not have proper tools or information to diagnose and solve problem on location.

The major means of mitigating these risks, and the controls needed to implement an effective antivirus system, would be as follows:

- As already mentioned, effective policies need to be written and put in place for enterprise-wide understanding of management's stance on virus protection.
- Information Security education and training needs to be developed to enable users and IS staff to assist in remedying the malicious code problems they encounter.
- Centrally managed antivirus software needs to be installed on all end-user machines and servers.

- Antivirus software needs to be installed/configured on the email gateway and effectively managed to reduce the threat of infection via email.
- Tools and procedures need to be made available to the Field Services team for effective local remediation.
- Communication to/from the Help Desk needs to be ensured for effective process flow.

In terms of controls that are defined within the ISO 17799 standard, the following might apply:

- 3.1.1 and 3.1.2 – Creation of a security policy document (relative to viruses and malicious code), and the review and evaluation of this document.
- 6.2.1 – Information security education and training, where all relevant users of enterprise systems are trained for what to look for with regards to malicious code.
- 6.3.1 – Reporting of security incidents, where a defined channel is available for employees to report possible/suspected malicious code outbreaks and infections. This will also include "backup" methods of reaching the Help Desk.
- 8.3.1 – Control against malicious software. This will be a technical control that encompasses the installation and maintenance of all antivirus software in the enterprise.
- 11.1.x – Business Continuity Management. Controls and procedures should be in place to ensure that interruptions in communications between users and the Help Desk are planned for, and testing of these procedures is consistently done to make sure the organization is prepared in case of an emergency or outage.

III. Do

Now that the needed improvements in the antivirus system have been identified, it is time to lay out a set of steps for each improvement.

1. Create an effective antivirus security policy

Problem: The organization does not have any existing security policies. As such, no enterprise-wide policy exists that mandates antivirus software must be installed or configured.

Action: This will be addressed by creating a security policy for antivirus within the organization.

Steps:
--Step one: Form an information security committee to discuss policies and procedures.

--Step two: Draft an information security policy pertaining to corporate antivirus software and strategies.
--Step three: Finalize the policy, with upper management approval.
--Step four: Publish the policy and make it accessible to all company employees.

2. Install antivirus software on all appropriate systems

Problem: Centrally managed antivirus software needs to be installed on all end-user machines and servers. Also, antivirus software needs to be installed on the email gateway and effectively managed to reduce the threat of infection via email.

Action: After determining which software to use, based on licensing and effectiveness, antivirus software should be installed and configured on end-user machines, servers, and the company's Microsoft Exchange server. Some of this software exists currently, and only needs to be upgraded and/or configured.

Steps:
--Step one: Evaluate current software, and determine whether existing products are working well or whether we need new products.
--Step two: Upgrade products, purchase new products, etc.
--Step three: Install products on all systems, using different vendors' products for multi-tiered defense.
--Step four: Document all configurations and create procedures to accompany policy.
--Step five: Install any centralized consoles available to allow the Help Desk or other support staff to monitor and configure end-user antivirus software.

3. Develop information security awareness training

Problem: Information Security education and training needs to be developed to enable users and IS staff to assist in remedying the malicious code problems they encounter.

Action: Develop an awareness program and integrate this into HR's standard hiring procedures. Develop some guidelines for yearly maintenance of this training for each user.

Steps:
--Step one: Draft information security awareness tips pertaining to antivirus software and viruses in general, and discuss with Security Committee.
--Step two: After agreement from the Committee, finalize the antivirus awareness training material and integrate into the overall Awareness program.
--Step three: Ensure that communication methods to the Help Desk are listed in the training material, and check to make sure they are being used.

4. Provide Field Services team with necessary resources to eliminate malicious code on local systems

Problem: Field Services staff are not equipped or trained to effectively eliminate malicious code from systems known to be infected.

Action: Create a shared network area containing tools and procedures for the Field Services staff to make use of.

Steps:
--Step one: Create a shared network folder that the Field Services team can access from anywhere in the network.
--Step two: Create folders here that are named after viruses. In these folders, place fix tools and registry hacks that repair systems from virus infections.
--Step three: Include in the shared area a document that lists, by virus name, the step-by-step procedures for removing the infection.
--Step four: Keep the most current patches, hotfixes, virus definition files, etc. in this area as well, and maintain the area (keep files current).

Now we can develop Statements of Applicability for the controls we have opted to implement and those we haven't. An example of one of the controls we WILL implement for the antivirus system is as follows (2):

Statement of Applicability for Company X Antivirus System

Implement: Fully
Justification for partial or non-implementation: Not applicable

8.3 Protection against malicious software
8.3.1 Control against malicious software

Control Reference	Description	Implement	Justify	Method	Comment
8.3.1	Detection and prevention controls to protect against malicious software and appropriate user awareness procedures shall be implemented.	Fully	N/A	Refer to Corporate Antivirus Policy and Procedure	End-user, server, and email server antivirus software will be installed.

This would be an example of the SoA that would be implemented in our system. For a control that would not be implemented in the antivirus system, the following example is given (2):

Statement of Applicability for Company X Antivirus System

Implement: No
Justification for partial or non-implementation: Not applicable

9.2 User Access Management

9.2.1 User Registration

Control Reference	Description	Implement	Justify	Method	Comment
9.2.1	Whether there is any formal user registration and deregistration procedure for granting access to multi-user information systems and services.	No	N/A	N/A	No registration is required for antivirus software, and there will be no general user access.

IV. Check

The first three items above will have auditing checklists created for compliance checks. The fourth item, creating documentation and a file share for the Field Services team, will not be covered. All of the following checklists have information derived using the SANS ISO 17799 checklist (1).

Security Policy Checklist (1)

The security policy for the antivirus system portion of the organization's ISMS has been written and included in Appendix A.

Reference: 3.1.1	**Audit area:** Information security policy document	
Audit Question		
Whether there exists an Information security policy related to antivirus software and malicious code management, which is approved by the corporate management, published and communicated as appropriate to all employees. Whether it states the management commitment and set out the organizational approach to managing information security (specific to antivirus systems).		
Reasoning/Importance of control		
The existence of an information security policy pertaining to installation, maintenance, and control of antivirus software in the enterprise is important. Letting employees know the expected actions to take and communications that are required upon possible malicious code infection will foster consistency in prevention within the organization.		
Expectations for compliance		
The security policy for antivirus exists and is available to all company employees in both written and electronic form (via Intranet). The policy is effective and makes sense in the organization.		
Audit steps/procedures	**Findings**	**Compliance**
1. Check to see if policy exists, and has been signed off on by upper management.	Policy exists	**Yes**
2. Policy is included in written policy handbook and available to all employees upon request.	Policy is included in employee policy handbook.	**Yes**
3. Policy is available from the corporate Intranet, found by clicking simply in the "Information Security" section of the Information Systems Dept. page.	Policy is posted in HTML format on the corporate Intranet.	**Yes**
4. Policy is easily understood and enforceable. This can only be assessed objectively by evaluating employee response to the policy.	Employees have complied with the principles in the policy.	**Yes**

Reference: 3.1.2	**Audit area:** Review and Evaluation (policy document)	
Audit Question		
Whether the Security policy has an owner, who is responsible for its maintenance and review according to a defined review process. Whether the process ensures that a review takes place in response to any changes affecting the basis of the original assessment, example: significant security incidents, new vulnerabilities or changes to organizational or technical infrastructure.		
Reasoning/Importance of control		
The information security policy must be updated to reflect possible changes in malicious code management strategies (in the industry or in general), as well as possible organizational changes that may be relevant.		
Expectations for compliance		
The organization's antivirus policy is reviewed on a regular schedule by a designated policy 'owner', and changes are made based on need.		
Audit steps/procedures	**Findings**	**Compliance**
1. The antivirus information security policy has a defined owner who is responsible for regular review and maintenance.	Corporate information security manager, Dave Shackleford, is responsible for review and maintenance of the policy.	**Yes**
2. The policy is reviewed on a regular schedule.	The policy is reviewed on a quarterly basis by Dave Shackleford, and every 6 months by the Information Security Committee.	**Yes**
3. Changes affecting the antivirus policy are recorded prior to review, and considered during policy review.	All changes are maintained in a policy review change log, and introduced during formal review sessions.	**Yes**

Antivirus software Installation/Configuration Checklist (1)

The antivirus software decided upon in the company is 3-tiered:

- On end-user systems (desktops, laptops, etc.), Symantec Client Security (formerly Norton Antivirus Corporate Edition) version 8.1 is installed. 3 servers have been installed as dedicated Symantec servers that service client requests, maintain configurations, provide updated definition files, etc. A centralized console has been installed (using the Symantec System

Center) for review by Information Security staff, Systems Administration staff, and the Help Desk.

- On servers, McAfee VirusScan 7.1 has been installed. The clients all pull updates from one of two central virus definition repositories (created using McAfee Autoupdate Architect). This provides an automated solution that requires little maintenance and maintains daily definition file updates to all clients.
- The email server, running Microsoft Exchange 2000, has Trend Micro Scan Mail 6 installed. This is configured to delete all file attachments other than ZIP files (used by executives, an accepted risk), and updates definition and engine files every hour.

<table>
<tr><td><b>Reference:</b> 8.3.1</td><td colspan="2"><b>Audit area:</b> Control against malicious software</td></tr>
<tr><td colspan="3"></td></tr>
<tr><td colspan="3" align="center"><b>Audit Questions</b></td></tr>
<tr><td colspan="3">Whether there exists any control against malicious software usage.
Whether the security policy does address software-licensing issues such as prohibiting usage of unauthorized software.
Whether there exists any Procedure to verify all warning bulletins are accurate and informative with regards to the malicious software usage.
Whether Antivirus software is installed on the computers to check and isolate or remove any viruses from computer and media.
Whether this software signature is updated on a regular basis to check any latest viruses.
Whether all the traffic originating from un-trusted network in to the organization is checked for viruses. Example: Checking for viruses on email, email attachments and on the web, FTP traffic.</td></tr>
<tr><td colspan="3" align="center"><b>Reasoning/Importance of control</b></td></tr>
<tr><td colspan="3">This control mandates that antivirus software exists and is the licensed and approved corporate standard. The control also ensures that procedures are in place for updating the software's virus signatures, viruses are contained appropriately, and that other specific types of traffic are checked for malicious code.</td></tr>
<tr><td colspan="3"></td></tr>
<tr><td colspan="3" align="center"><b>Expectations for compliance</b></td></tr>
<tr><td colspan="3">Corporate licensed and approved antivirus software is the only software installed and configured on corporate computing property. The software is configured to alert users to the presence of viruses, download and install new virus definition updates, and effectively contain any malicious code detected. Email gateway antivirus software will scan all incoming and outgoing email messages for malicious code, and delete any files that are labeled as viruses, as well as any attachments other than ZIP files (the content of which is scanned).</td></tr>
<tr><td colspan="3"></td></tr>
<tr><td align="center"><b>Audit steps/procedures</b></td><td align="center"><b>Findings</b></td><td align="center"><b>Compliance</b></td></tr>
<tr><td>1. The approved end-user client antivirus software is installed on all users' personal computing machinery, including desktops and laptops. Open the Symantec System Center console by clicking Start→Run→"mmc". Then, click File→Add/Remove Snap-in, and click the "Add" button. Scroll down to "Symantec System Center", click "Add", and then click "OK". In the console window, review the listed computers for installed software reporting to the central servers.</td><td>All company machines are present in the Console directory, with antivirus software enabled.</td><td align="center"><b>Yes</b></td></tr>
</table>

2. The approved server-level antivirus client is running on each server, and updating from a central definition file repository. This must be checked on each individual server. A batch script has been written to send a log to a central location each night. The batch file is listed as Appendix B. The procedure for running this task as a Scheduled Task under Windows 2000 Server is as follows: a. Click Start→Programs→Accessories→System Tools→Scheduled Tasks. b. Double-click “Add Scheduled Task”. Click “Next”. c. Browse to “C:\ av_update_log_copy.bat”. d. Select “Daily”, and click “Next”. e. Enter the time as 4:00 AM, and click “Next”. f. Enter a username and password with proper privileges on the server to execute this task. g. Click “Finish”.	Each server is updating virus definition files daily from a central location. This is easily checked by reviewing the update logs every morning.	**Yes**
3. The email gateway antivirus software is installed and configured to update definitions hourly. This can be checked by performing the following: a. Log into the Microsoft Exchange server. b. Click Start→Programs→Trend ScanMail for Exchange→ScanMail Management Console. c. Enter the proper authentication credentials (username and password). d. Select the “Active Update” tab on the left-hand side. e. Select “Scheduled Update”. f. Ensure that the “Enable Scheduled Update” checkbox is selected, and the selection box is set to “Hourly”. g. Make sure that the Update location is set to: http://smex-t.activeupdate.trendmicro.com/activeupdate	The email gateway’s antivirus protection is installed and configured to receive hourly updates of both definition files and scanning engine files.	**Yes**
4. The email gateway antivirus software is configured to delete any attachments other than ZIP files. This would include the following attachments: PIF, SCR, BAT, EXE, COM, and CMD. Check this by: a. Clicking the “Virus Scan” tab on the left-hand side, and selection the “Options” button. b. Ensure the “Enable attachment blocking” checkbox is selected. c. Click “Settings” next to the attachment blocking checkbox. d. Ensure that the “Specified attachments” button is selected, and the extensions listed previously are in the message window, separated by semicolons. e. Ensure that the “Action on file attachments” option is set to “Delete”.	The email gateway antivirus software is configured to delete all attachments with the extensions PIF, SCR, BAT, EXE, COM, and CMD.	**Yes**

5. The contents of compressed ZIP files are scanned 6 levels deep. This is checked by: a. Clicking the “Virus Scan” tab on the left-hand side, and selection the “Options” button. b. Checking the checkbox under “Advanced Options” that is labeled “Scan compressed attachments”. c. Set the “Scan compression layer” setting to “6”.	The email gateway antivirus software is configured to scan 6 layers into compressed ZIP files.	**Yes**
6. Make sure that the email gateway antivirus software alerts administrative staff to an outbreak alert. This is checked by: a. Clicking the “Notification” tab on the left-hand side, and selection the “Outbreak Alert” button. b. Check the checkbox that reads “Enable Outbreak Alert when viruses found exceed” and change the value to “200” in a 24-hour period. c. Check the box that reads “Windows Event Log”.	The Windows Event Log is recording the presence of any potential outbreaks on the Exchange server.	**Yes**
7. Make sure that the Symantec antivirus servers alert administrative staff to an outbreak. Check the AMS (Alert Management System) service on each server by: a. Clicking Start→Programs→Alert Management Server→AMS Admin utility. b. In the console that opens, select the “Local AMS Server” button, and click “Configure AMS”. c. Open the “Norton Antivirus Corporate edition” tree, and select the “Virus Found” option. d. An alert should exist to send Internet mail with the following options: --- Alert: Virus Found Date: <Date> Time: <Time> Severity: <Severity> Source: Norton AntiVirus Corporate Edition Virus: <Virus Name> PC: <Infected PC Name> User: <Logged on User Name>	The AMS service is set up on each Symantec Antivirus server to alert the administrators when a virus has broken out.	**Yes**
8. Make sure that the McAfee client software is logging virus infections on servers. This is managed via another batch script and log file (using Task Scheduler) as follows (script listed in Appendix B): a. Click Start→Programs→Accessories→System Tools→Scheduled Tasks. b. Double-click “Add Scheduled Task”. Click “Next”. c. Browse to “C:\ av_virus_log_copy.bat”. d. Select “Daily”, and click “Next”. e. Enter the time as 4:00 AM, and click “Next”. f. Enter a username and password with proper privileges on the server to execute this task. g. Click “Finish”.	The McAfee server clients are all copying the virus scanning logs to a central location.	**Yes**

<u>Information security awareness training checklist</u> (1)

The information security awareness program has a few guidelines and common sense bits of information that will assist personnel in making more informed decisions regarding how to handle potential virus infections. Also, the awareness training will include information on who to contact and how to reach them should the user have any concerns. The basic guidelines for users with regard to antivirus management is listed in Appendix C.

Reference: 6.2.1	**Audit area:** Information security education and training	
Audit Question		
Whether all employees of the organization and third party users (where relevant) receive appropriate Information Security training and regular updates in organizational policies and procedures.		
Reasoning/Importance of control		
End-users, or general company employees, are always the first line of defense in prevention; the more general knowledge these users have, the more they will be able to help in preventing, detecting and eradicating malicious code.		
Expectations for compliance		
Users have signed off on a paper form acknowledging that they have read the information security guidelines when they begin employment with the company. Also, employees must undergo yearly training that is electronic (in HTML format) on the company Intranet and indicate that they have finished the short program.		
Audit steps/procedures	**Findings**	**Compliance**
1. Have users received corporate policy handbook?	Users have physical handbooks.	**Yes**
2. Is there a sign-off sheet on file for all users (kept by HR)?	All users' employee files have the sign-off sheet included.	**Yes**
3. Is information security and awareness training available to all users on the company Intranet?	Information security training is available on the corporate Intranet.	**Yes**
4. Are users required to undergo "refresher" training each year and sign a form indicating that they have finished the course?	Users' training and sign-off forms are updated yearly.	**Yes**

<u>Security Incident Reporting checklist</u> (1)

It is extremely important that the Help Desk coordinate all malicious code incident response. As the central contact point/interface between the organization's users and the other IS staff, the Help Desk should be the first to be notified by users when malicious code or strange behavior (suspected malicious code) is detected. The Help Desk, in turn, should have a set of procedures and contact information in place to adequately handle any incidents and assist in getting them resolved in a timely fashion.

Reference: 6.3.1	**Audit area:** Reporting security incidents

Audit Question
Whether a formal reporting procedure exists, to report security incidents through appropriate management channels as quickly as possible.

Reasoning/Importance of control
The more streamlined and defined the virus/malicious code incident reporting mechanism is, the quicker and more efficient the IS Security team will be in mitigating the risks of infection and spread.

Expectations for compliance
The means of contacting the Help Desk is made available to all users, both on the corporate Intranet and phone list, and within the information security awareness training. The IS department has internal reporting guidelines and information.

Audit steps/procedures	**Findings**	**Compliance**
1. Is the Help Desk email address and phone number posted on the Intranet and readily available in the employee handbook and Outlook directory?	The Help Desk contact information is available in all locations, easily accessible.	**Yes**
2. Do the antivirus guidelines in the security awareness training direct the user to call the IS Help Desk in case of suspected malicious code activity?	The user is directed to call the Help Desk if a virus notification pops up, or if strange behavior is noticed on the system.	**Yes**
3. Does the Help Desk know how to operate the Symantec Antivirus Console and look up a user’s machine to check for viruses? Do they: a. Click Start→Run→”mmc”. b. Click File→Add/Remove Snap-in, and click the “Add” button. c. Scroll down to “Symantec System Center”, click “Add”, and then click “OK”. d. In the console window, look up the suspect computer name, and then right-click. Select “All Tasks” and “Symantec Antivirus”. e. Select “Logs”, and then “Virus History”.	The Help Desk is equipped with the Symantec System Center console, and is trained in looking up user machines and viruses.	**Yes**
4. Does the Help Desk have a defined call tree or escalation plan to contact the appropriate Field Services team members when malicious code needs to be eradicated?	The Help Desk has email addresses, phone and cell phone numbers, and pager numbers for the entire Field Services team.	**Yes**

IV. Act

Now, the basic antivirus component of the ISMS has been put in place. The systems are configured, and the staff and end-users are better-educated and trained in handling virus outbreaks and infections. The various ways to keep the system maintained and updated are as follows:

- Revise and update policies. The corporate antivirus policy, as well as the procedures and guidelines that accompany the policy, should be reviewed on a regular basis for relevance. The Information Security committee that was formed will review this policy every six months. The Information Security Manager will perform a more casual assessment of the policy every 3 months. Should the policy's alignment with organizational operations change, the policy and other documents will be revised to match the company's operating methodology.
- Evaluate the software and systems architecture for the antivirus system. As the company expands, more than 3 Symantec servers may be needed to handle client requests and definition file updates. Is Symantec doing an acceptable job in preventing and detecting malicious code? These concerns would apply to the other 2 levels of protection, the McAfee server-level clients and the Trend Micro ScanMail software. Each of these will be evaluated every 6 months. Trends will be created by measuring monthly virus activity and remediation percentages. Is the software preventing an acceptable percentage of malicious code infections? This will provide data for a malicious code baseline. The later numbers can then be measured against this baseline, and the configuration can be changed to improve the rate of prevention. If the rate does not improve to an acceptable level, determined by the Information Security committee, then new software will be evaluated.
- New means of centrally managing the solutions may improve the overall effectiveness and manageability of the antivirus system. The company has evaluated products such as McAfee E-Policy Orchestrator (EPO), which allows a central console to monitor and manage multiple antivirus products from different vendors.
- Improve the communications and incident handling procedures within the IS department. A baseline number of calls to the Help desk should be measured at the beginning of the system implementation. After implementing the antivirus system, the number of calls to the Help Desk should increase. Likewise, the number of virus incidents should decrease **overall**, as the response times for incident handling decrease. This will be a result of less spread of infection. Improving communications capabilities is important, and redundancy in telephone and email methods should be implemented.
- Improve response times. The Help Desk should begin recording the time from an incident being reported by user or alert to the Help Desk logging the issue with Field services as the Detect time. The time it takes for a Field Services technician to actually solve the problem should be recorded

as the Response time. The goals for these times are 1 and 3 hours, respectively. Improving these times should be a primary goal of the system, in order to reduce overall risk to the organization.

- Improve the quality of training for users. By making the training more interactive, using different multimedia methods, users will be more likely to “take something away” from the training.

References

1. Thiagarajan, Valliappan in conjunction with the SANS Institute. “ISO 17799 Checklist”. August 2003.
Available at: http://www.sans.org/score/checklists/ISO_17799_checklist.doc

2. Wilbert, Perri. “Getting Serious About Security, vol.5”. October 16, 2001.
Available at: http://security.kingsley.co.za/articles/soa.htm.

3.”BS 7799 – ISMS”. Author Unknown.
Available at: http://www.dnv.co.kr/Binaries/BS7799PRESENT-2002_tcm34-30701.pdf

4. Zuccato, Albin. “Risk Analysis”.
Available at: http://www.cs.kau.se/~albin/Documents/F18-RiskAnalysis.pdf

5. SANS Institute Security Policy Project.
Available at: http://www.sans.org/resources/policies/Anti-virus_Guidelines.doc

6. SANS Institute Security Policy Project.
Available at: http://www.sans.org/resources/policies/Lab_Anti-Virus_Policy.doc

7. Stoneburner, Gary, Goguen, Alice, and Feringa, Alexis. “Risk Management Guide for Information Technology Systems”. NIST, 2001.
Available at: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

8. SANS G17799 Course Material, Day 4. “Time Based Analysis”. Pgs. 94-109.

Appendix A – Antivirus Security Policy (6)

1.0 Purpose

To establish requirements which must be met by all computers connected to <Company Name> networks to ensure effective virus detection and prevention.

2.0 Scope

This policy applies to all <Company Name> computers that are PC-based or utilize PC-file directory sharing. This includes, but is not limited to, desktop computers, laptop computers, and servers of any type

3.0 Policy

All <Company Name> computers must have <Company Name>'s standard, supported anti-virus software installed and scheduled to run at regular intervals. Non-server systems will use a managed client, with virus definition files installed automatically. All software will be installed by members of the IS Department.

Any user detecting a virus via software alert or other virus-indicative behavior (see <Company Name>'s *Anti-Virus Recommended Processes*) must call the IS Help Desk to report it. Virus-infected computers must be removed from the network until they are verified as virus-free. The MIS Security Administration team is responsible for creating procedures that ensure anti-virus software is run at regular intervals, and computers are verified as virus-free. Any activities with the intention to create and/or distribute malicious programs into <Company Name>'s networks (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are prohibited, in accordance with the *Acceptable Use Policy*.

Refer to <Company Name>'s *Anti-Virus Recommended Processes* to help prevent virus problems.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Revision History

Appendix B – Scripts for replication of server antivirus logs

Script 1: av_update_log_copy.bat

```
copy "C:\Documents and Settings\All Users\Application Data\Network
Associates\VirusScan\UpdateLog.txt" \\<servername>\<directory>\av_log-
%computername%.txt
```

Script 2: av_virus_log_copy.bat

```
copy "C:\Documents and Settings\All Users\Application Data\Network
Associates\VirusScan\OnDemandScanLog.txt"
\\<servername>\<directory>\av_scan_log-%computername%.txt
```

Appendix C – Anti-Virus Recommended Processes (5)
(as part of security awareness program)

- NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.
- If possible, disable your “Preview Pane” and “Auto Preview” features in Microsoft Outlook.
- Delete spam, chain, and other junk email without forwarding, in with <Company Name>'s *Acceptable Use Policy*.
- Never download files from unknown or suspicious sources.
- Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.
- Always scan a floppy diskette from an unknown source for viruses before using it.
- Back-up critical data and system configurations on a regular basis and store the data in a safe place.
- Information about new viruses can usually be found from links posted on the <Company Name> Intranet, in the IS Department under “Information Security”.
- When a pop-up box from your antivirus application appears on your system, immediately call the IS Help Desk at extension 7221, or send an email to help@<company>.com. Also contact the Help Desk if your system is behaving oddly or in a suspect fashion.