Developing an Anti-virus Security Policy

An IT Security Policy is aimed at protecting the Confidentiality, Integrity and Availability of resources, data and programs. Essentially, it will:

* Define what you want to protect
* Analyze what it is you want to protect it from
* Explain how you intend to protect it

To be effective, it must be both holistic and dynamic. To be achievable, it must be realistic in its goals and (where user conformity is required) expressed in a way that is simple and short enough to ensure it is read, understood and followed.

The overall security policy will address such areas as:

* \* Physical security of your data and systems
* \* Access control to your data and systems
* \* Data integrity and availability
* \* Contingency and recovery plans (Disaster Recovery, Failover, Backup Recovery)

Anti-virus issues are simply one element of such a policy - viruses are one of the risks this policy must protect against.

The information that follows addresses this anti-virus component. To provide context, it includes considerations that would properly be covered at a higher level of an overall policy.

The information presented is necessarily generic, and is not intended to be exhaustive - the content of any security policy ultimately rests with its author. However, this paper does provide a starting point for writing such a policy.

The process is broken into two sections:

1. Risk Analysis: A brief look at this fundamental building block of any site security policy, concentrating only on the viral and related component of risk
2. Security Policy: Outlines how to build the security policy, using the information gathered in the Risk Analysis

Defining Your Security Risk Exposure

Each of these sections is covered in detail below.

Operating Environment

Here we define the environment within which the business operates. This allows us to assess sources of vulnerability both within and to that environment.

For the purposes of this paper, our list will be limited to the computing environment, as this is where we are vulnerable to viruses.

The assessment will cover both the physical elements and the "control" issues of this environment.

The following lists suggest areas to be considered:

Physical Elements:

* Platforms (Intel, DEC, Macintosh, etc)
* Operating Systems (DOS, Windows (all), NetWare, UNIX, etc)
* Hardware (Dumb Terminals, Diskless Workstations, Desktop Systems, etc)
* Software (Off-the-shelf, Customized, Internally Developed, Non-business (e.g. games), etc)
* Communications (Network Types, Modems, other links)

"Control" Issues:

* Standardization
* What is the level of server standardization?
* What is the level of desktop standardization?
* Users
* What is the level of user competence in terms of security issues?
* What controls are in place to ensure and monitor staff conformity to security policy?
* Externals
* Define our reliance on contractors, solution providers etc (for hardware and software)
* Define our reliance on external data and service providers (e.g. ISPs, stock-market feeds etc)
* Define what other external services and data we accept (news feeds, general downloads etc)

Business Systems

Armed with a broad overview of our system, we now turn to the specific components of our business system that need to be protected. Viruses directly threaten a company’s data and computer based services, and indirectly their reputation.

Our task is thus to list all data and computer based services provided by or necessary to the company’s existence. The list will include, but not be limited to, objects from the following areas:

Internal Records

* Databases
* Spreadsheets and other financials
* Documentation
* Product and services information
* Employee information
* Strategic plans (by category/department)
* Any other sensitive and/or confidential information (by category)

Electronically Provided or Supported Services

* Electronic order acceptance and Customer subscription services
* Information services

External "Product"

* "Data feeds" from external sources
* Access to external services necessary to run the business

Vulnerabilities

In this section, we examine the specific vulnerabilities inherent in how we do business. The analysis is broken into a number of parts, each of which follows on from those preceding it.

Threats

A threat is a general danger to the viability of our business. As we are confining our discussion to threats associated with viruses, which primarily target our systems and data, our threats may be limited to the following:

* Threats to data
* Threats to systems (software, communications, services)
* Threats to reputation
* Threats to finances

Vectors of Threat

In the wider scheme of things, this is where we would list all of the ways the above areas are threatened. Thus, while our focus is on the threat to our data from viral incidents, normally we would also identify our data being vulnerable to damage by anything from a major disaster, such as a fire or flood, through more common occurrences, like a hard drive failure, faulty cable, power interruption and simple user error.

This is also the place to identify how a vulnerability threatens us - i.e. its vector of attack. It is not enough to identify the susceptibility of our systems to a virus attack as a vulnerability - we also have to understand how viruses gain access to our systems, so that we can take measures to keep them out.

Our pre-work in defining the operating environment helps us here - it limits our list of vulnerabilities to those that target that environment.

Level of Exposure

Here we define how exposed the business is to each of the threats identified. This is driven by an examination of the operating environment and the vectors of attack that threaten it, and is highly business specific. A sample (and cut-down) analysis is given below:

1. Threat
2. Vector
3. Exposure

Boot Sector Virus

1. Boot from Infected USB
2. Run infected file
3. Medium - networks, intranet and CDs have reduced the number of floppy disks in use
4. Medium - Win3x environment; uncontrolled use of files from various sources, but number of such viruses considered relatively low

Executable File Viruses

1. Load and execute infected file
2. High - uncontrolled use of files from various sources.

Macro Viruses

1. Load infected Word Document
2. Load infected Excel Spreadsheet
3. High - All business units exchange Word documents internally and externally.
4. Low - no exchange of Spreadsheets

Trojans

Run Trojan file

Medium - uncontrolled use of files from various sources, but exposure to Trojans considered low Hoaxes Chain-letter effect High - extensive use of e-mail and News Logic Bombs Coded into custom programs Low - low use of contractors; satisfied staff Figure 3: Level of Exposure

Consequences of Threat

Having defined the areas that are threatened, and our exposure to viruses as a vulnerability that would realize those threats, we can combine the two to list the potential consequences of a virus infection.

Threat

Vulnerability

Threats to data: Direct action of virus on data integrity. Downtime while infection/rumor is cleaned/investigated. Suspension of essential/useful/non-essential internal and external services. Time to restore from backups/rekey data/check data integrity:

* Data destroyed/corrupted
* Access to data suspended
* Data exposed to world
* Boot Sector, File, Macro virus, Logic Bomb & Trojan
* All

Threats to systems (software, comms, services): Software necessary to running systems corrupted/destroyed. Downtime while infection/rumor is cleaned/investigated. Suspension of essential/useful/non-essential internal and external services.

* \* Systems destroyed/unreliable
* \* Access to systems suspended
* \* Systems exposed to world
* Boot Sector, File, Macro virus, Logic Bomb & Trojans
* Advanced / Complex threats

Threats to reputation: External world learns of virus infection or its consequences.

* \* Business seen as insecure
* \* Business seen as uninformed
* Boot Sector, File, Macro virus, Logic Bomb & Trojans
* Hoaxes
* Advanced / Complex threats

Threats to finances: Costs associated with dealing with the threat

* \* Cost of cleaning infection/repairing consequential damage/recovery
* \* Cost of interruption to services
* \* Legal costs due to suspension of services, infecting clients etcetera

Consequence of Threat

Clearly, at this level the analysis will be highly dependent on the individual business. The above are simply some of the areas that need to be considered.

Impact Assessment

This is the final piece of the risk assessment. Having identified what our business areas are, and the threats to those areas, we now need to determine what impact it will have on our business if one of these areas is compromised.

Here impact is assessed in terms of the categories of "damage" that could be done to each data set and service identified. Some of the possible "damage" categories are listed across the top of

The actual impact assessments are purely notional - they will vary by company.

* Object
* If destroyed
* If altered/corrupted
* If exposed
* If suspended
* Other

Business Impact Analysis

A true risk analysis would also include some indication of the size and type of investment an object represents, and its "replaceability" should it be lost, along with the general impact assessment. The depth of analysis required for this section will be governed by the complexity and needs of the business.

Where different business units come to different impact assessments on the same object, always record the highest impact.

The Anti-Virus Security Policy

Having identified the components of, and threats to, our system, our next step is to create the policies that will protect our business.

For the purposes of this discussion the "padding" that should go with this policy (Introduction, Statement of Purpose, Background, Context Statement, Definitions, Governing Policies, etc) are assumed.

The focus of this section of the paper will be exclusively on developing the anti-viral component of a Security Policy.

Define the Security Goals

Our goal will be governed by the potential business impact of each virus risk identified, and the cost of managing that risk. Some companies may not be able to risk any possibility of a virus infection, and will set extremely high anti-virus security goals; for others it may be cost-effective to deal with the infections as they arise.

The key issue here is to balance the effort and cost required to keep viruses out against the business exposure to viruses and the potential impact of a virus incident identified in the risk assessment.

Our goal will fall somewhere in the following broad spectrum:

* No virus incidents
* All viruses detected and contained at the perimeter of the business environment
* All viruses detected and contained as soon as they enter the business environment
* X% of viruses detected and contained as soon as they enter the business environment; virus incidents caused by the (100-X)% that escape initial detection handled according to our security policy
* Viruses incidents are an accepted part of the business environment

Define General Duties and Responsibilities

Generally, ultimate responsibility for the anti-virus policy and implementation lies with whoever writes the security policy document, though this is not always the case. It is important that this person/department is identified and given sufficient authority to achieve the goals of the policy.

At its most basic, the following duties and responsibilities will exist within most companies (though the actual hierarchy may differ significantly):

* Person/Group
* Duty
* Responsible to:

Information Security Manager

* Design Policy
* Management Team

Information Security Department

* Implement Policy
* IS Manager

Help Desk

* Teach and Support Policy
* IS Manager

Users

Follow Policy Help Desk/Security Manager In the above model, the IS manager and their team select, implement and support the suite of security packages they have chosen to drive this policy, ensuring both the policy itself and the packages chosen to implement it are kept up to date.

The role of the help-desk is to ensure the policy is understood, followed and supported. This is a typical approach that places responsibility with the experts and frees the users to get on with their jobs.

(The specific responsibilities (expected actions and behavior) of the users are discussed in section 5 of this paper)

Define the Security Baseline

The baseline defines our minimum-security implementation.

For simple ease of management, it would be ideal if we could define and implement a single baseline for the entire company; in practice, the number and diversity of systems and business units may make this impossible.

The baseline will derive from the information discovered in the risk assessment, and may require changes to our operating environment. Figure 6 lists some of the areas that might be considered along with a selection of potential policy decisions, and some consideration of the gains and costs of implementing each. A more complete analysis would also list the gaps left open by the baseline.

Please note below is not intended to be an exhaustive listing of security alternatives, but simply a starting point for consideration of the security alternatives available.

It is also to be noted that both the baseline and additional security sections will give some indication of how often they should be reviewed and updated.

* Area
* Selection of Potential Policy Decisions
* Gain
* "Cost"

Select a network that provides secure login and access restrictions (and use same)

Allows logical separation of data and programs. Can block file viruses from writing to executable file areas

Increased administration; cost of hardware and OS etc

Software

Define and enforce company standards for desktop and servers

Simplifies management of environment; potentially reduces virus risk (e.g. select non-MS Office applications to avoid current macro viruses) May lose functionality/ interchangeability.

Install a good end point AV automatic and on-demand virus protection software at the desktop Detects and cleans of viruses as they enter the business environment

* Cost of software
* Managing roll-out of updates

Install a good end point AV automatic and on-demand virus protection software at the server level

Creates a choke point. Detects and cleans viruses as they enter the business environment

* Cost of software
* Managing roll-out of updates

User Behavior

Require all files and disks brought to work/downloaded etc to be checked at central point

Creates a choke point to prevent virus entry into the business environment

Staff to manage same

Cost of software etc to do the checking   Establish awareness and reporting procedures, etc Creates an environment where users are actively taking steps to prevent, recognize and control virus outbreaks Education and awareness campaigns Help desk to support same Figure 6: Establishing an Anti-Virus Security Baseline

Define Additional Security Measures

Additional security measures aim at controlling the "high-risk" areas of the business identified in the risk analysis. These may address applications that have been identified as open to particular attack, business-critical units, and responses to particular types of threat.

For example, a good end point AV for MS Exchange, is specifically targeted at closing exposure to viruses attached to e-mail messages.

Clearly the distinction between the security baseline and additional security measures will be highly company specific. Any of the alternatives may be reserved as additional security measures, just as the additional controls listed below could be implemented as part of the security baseline.

Potential choke points include:

* Connections to the outside world (force all such connections through controlled, shared modems, rather than allowing individual users their own modems)
* Controlling all software that comes into the company (by defining and enforcing a standardized desktop for instance)

Some specific risks that will be managed by our additional security measures include:

* Laptops/mobile users (unless tightly controlled exist outside the security perimeter)
* Contractors/Service personnel/Suppliers etc
* Downloaded software
* Disks, programs, documents brought from outside the office
* Unauthorized software
* Deliberate attacks