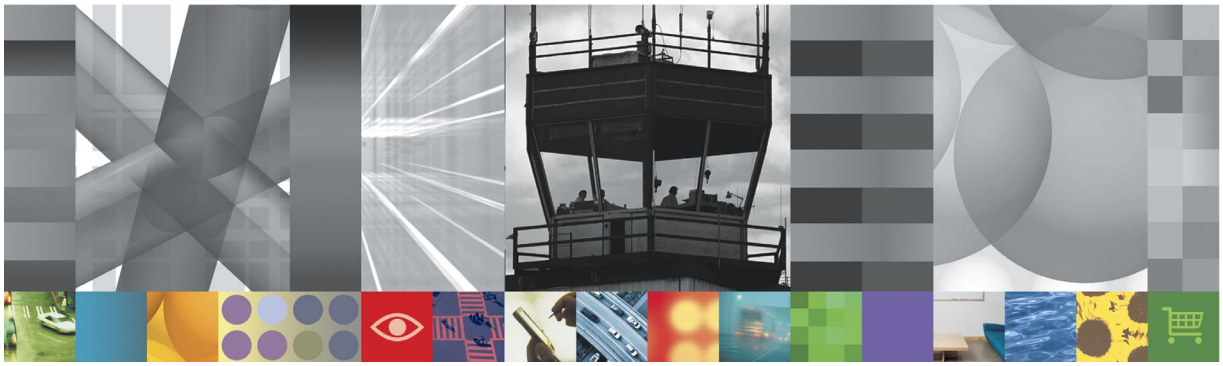
# IBM Start Now Infrastructure Management Solution

**Demonstration Script**

**English**



# Table of Contents

This document provides you with information on the demo provided with this solution. For details on how to recreate the demo for a customer engagement or in another language, go to the Demonstration Creation Document (IM_DemoCreation.doc).





# Introduction to the Demo

The demo included as part of the Solutions Guide is an **AVI** file. Home Abroad's website is up and running. They now have a successful e-business site selling goods to customers through the Internet. However, their concern is to provide not only an excellent shopping experience, but also a secure one. News reports of hackers stealing credit card numbers and internal threats worry the executives.

Home Abroad's information technology lead sponsor calls an IBM Business Partner who, after administering an assessment of the company's assets, explains the major components of security. The Business Partner proposes a security architecture and some guidelines on setting policies and procedures. Part of the security implementation is the installation of a security management system that centralizes the efforts of the intrusion detection system.

The Business Partner provides a visual presentation of security management featuring the IBM Tivoli Intrusion Manager product, where it fits in the physical topology, and the security architecture. The Business Partner also shows how IBM Tivoli Intrusion Manager has sensors at various points that report events to the Intrusion Manager central console. The Home Abroad information technology lead sponsor has the proposed security architecture deployed and a Home Abroad employee uses the IBM Tivoli Intrusion Manager product to analyze an event that has occurred when another employee receives a virus contained in an e-mail.

IBM Tivoli Intrusion Manager signals an event. The Home Abroad employee tracks this event, responds with the appropriate procedures that have been put into place, and alerts the company to the presence of the virus. A sample report shows events gathered from separate sensor points and lets the Home Abroad employee know what events have transpired. Reports may be generated based on different categories.



# Play the Demo

Follow these instructions to play the demo:

1. An **AVI player** is required to play the IBM Start Now Infrastructure Management Demo. A player such as Windows Media Player, RealNetworks RealPlayer, TechSmith Camtasia Player or any AVI player of your choice can be used.

2. The TechSmith Camtasia Codec file is required and is included with the IBM Start Now Infrastructure Management Demo. Run the "**tscc.exe**" file to install the codec.

3. Play the Intrusion Manager demo avi file. Double-click on the **.avi** file to begin playing.

   **Note:** If you choose the Camtasia Player software, it can be downloaded for free from the following TechSmith web site:
   http://www.techsmith.com/

4. Read the Demo Speaker Notes as an accompaniment to the automated demo.



# Demo Speaker Notes

This demonstration illustrates the Infrastructure Management solution concepts. It will introduce you to the solution, the scenarios, the products and some of the functionality that they provide. This visual demonstration will provide a means to help you quickly understand the solution area and scenarios as well as provide a mechanism to show your customer what the Infrastructure Management solution can do for his business.

Let's start!

**Slide 1** **"Start Now Infrastructure Management Solutions":** Welcome to the Start Now Infrastructure Management demonstration.

**NOTE:** This page may be edited or deleted, and your logo can be added.

**Slide 2** **"[Your Company Name Here]":** These are some real-world examples on how companies across the world have been hacked. If these companies can be hacked, so can you. There is a reason to be worried and there is a threat out there that should be taken seriously.

**Slide 3** **"Are You Concerned?":** Here are some questions to assess your security situation. The answers to the questions will determine what services I can provide for you. (*Read the questions to the customer*)

**Slide 4** **"Are You Next?":** Statistics show how common it is to be attacked by hackers or infected by viruses. This is a common problem, and there are some consequences associated with it.

A recent survey, from CSI, reported that 90% of respondents detected computer security breaches in the past 12 months. Of those respondents: 80% acknowledged financial losses due to computer breaches, 44% quantified their combined financial losses at over $4 million dollars, and 74% cited their Internet connection as a more frequent point of attack than their internal systems.

In addition, since January 2002, e-mail viruses are up 42%, with one in every 134 messages containing malicious code. And in a recent month, the number of website defacements reached an all-time high, with 9,000 attacks in one month, according to a London security consultancy - an increase of 54% from the prior month, also a record high.

**Slide 5** **"Key Losses":** Let me highlight three types of losses you can suffer from an attack to your company:

- **Direct financial loss -** This type of loss is a direct measurable loss of money. For example, loss could be due to fraud or theft.
- **Indirect loss -** An indirect financial loss is more difficult to measure because the loss is based on potential lost revenue and not an actual monetary figure. An example of indirect financial loss would be the lost revenue from your website being down for a day due to an attack and the additional labor costs to fix the problem.
- **Image Loss -** Adverse publicity is potentially the most costly, especially through loss of customers. Adverse publicity, or loss of image, is represented by the loss of trust your customers have in your business. If your company suffers a loss from a security mishap, your customers may decide to switch loyalties. A small or medium business is more vulnerable because they are usually beginning to build a reputation as a safe business. Customers may be more apprehensive to continue using your product or services if security is breeched, especially in a financial environment.



**Slide 6** **"Steps to Implement Infrastructure Management":** Let me show you how to get started in securing your e-business:

1. Perform a security assessment
   - Gather information about your business, such as infrastructure policies and procedures, and determine the relationships between departments that should or should not be set.
   - Perform a security audit by analyzing the system for potential vulnerabilities.

   This task establishes where you may have vulnerabilities or holes in your infrastructure.
2. Protect your e-business
   - Segment your infrastructure by implementing firewalls to improve your network security, control the access to the Internet, and ensure the continuity of business operations.
   - Protect against virus infection by installing anti-virus software on desktops, servers, and Internet gateways to avoid virus infection and spreading as well as mitigating the impact of viruses.
   - Identify and manage intrusions in your infrastructure. This will help you identify suspicious events and correct previously unknown exposures.

   With the above-mentioned tasks, you can optimize the security of your infrastructure system.

**Slide 7** **"An Unmanaged Infrastructure":** Here is an example of an unmanaged infrastructure that is unprotected against attacks from the outside. There is no protection in place against malicious code, such as viruses, or any outside intrusions from attackers. Also, system-wide monitoring of attacks and viruses does not exist.

**Slide 8** **"Protecting Your e-business":** By following the steps suggested earlier, the infrastructure is now more secure. Anti-virus software was installed on all servers and workstations, and firewalls were implemented to separate Web servers from the internal network and protect the company from outside intruders. But how do we monitor the infrastructure?

**Slide 9** **"Active Monitoring of Intrusions":** IBM Tivoli Intrusion Manager provides a centralized monitor to gather information from different sensors in the infrastructure. It then collects and correlates them. This helps by:

- Consolidating alarms received from many sources to a single console
- Saving time required to maintain and monitor several different logs
- Reducing administrative costs due to the difficulty in finding root causes of problems

**Slide 10** **"Virus Attack":** Let's take a look at a live attack of an infrastructure. Here is an illustration of a company network with anti-virus software, firewalls, and IBM Tivoli Intrusion Manager. In the internal network, there is a user desktop and an Intrusion Manager Console. In this scenario, a user receives an e-mail with an attached virus.

**Recorded Video 1** **"User opens mail with virus":** Here we will see how the virus attack occurs and how the console is alerted.



Betty opens her mail, reads a message, and launches an attached file. At that time, Symantec AntiVirus configured for "Real time" protection catches the virus hidden in the extracted file and reports that the anti-virus program has found a virus on the computer.

**Slide 11** **"Virus Alert":** We have just seen what happens on a protected desktop when a virus is detected. Let's see what happens next:

- The attack of the virus is reported to the IBM Tivoli Intrusion Manager Server as an event.
- The event is correlated and analyzed by the IBM Tivoli Intrusion Manager engine.
- The IBM Tivoli Intrusion Manager Console is updated to show a new alert.

**Recorded Video 2** **"Helpdesk Looks at the IBM Tivoli Intrusion Console":** Let's take a look at the alert as it appears on the IBM Tivoli Intrusion Manager Console of the helpdesk employee. After logging in, the helpdesk employee sees that a new incident has occurred on the console. To get more information about the incident he or she selects the **Problem Manager** and gets all of the details from the event by looking at the **Problem Report Details**. An e-mail is then sent to all employees to make them aware of the potential virus threat and remind them to verify they have the latest version of the anti-virus software.

Because of this implementation and these products, the company was protected from a potentially costly security problem.

**Final Chart** This is the conclusion of the IBM Start Now Infrastructure Management Solutions demonstration.