"Whether you are managing an existing NAVCE 7.6 configuration or implementing SAVCE version 8.*x*, this book will help you get the most out of your software installation…"
—**David Banes, Symantec Security Response, Asia Pacific Regional Manager**

SYNGRESS®

CONFIGURING Symantec™ AntiVirus Corporate Edition

Develop an Effective Enterprise AntiVirus Solution!

- Complete Coverage of Symantec System Center (SSC) Console
- Prepare for the Symantec Product Specialist (SPS) Certification Exam 250-011
- Master the "Three Cs" of Virus Response: Containment, Cleanup, and Communication

Laura E. Hunter
Athar A. Kahn
James Stanger, Ph.D.
Jay Cee Taylor
Robert J. Shimonski Technical Editor

SYNGRESS®

Configuring Symantec AntiVirus Corporate Edition

Laura E. Hunter
Athar A. Khan
JayCee Taylor
James Stanger, Ph.D.
Robert J. Shimonski, Technical Editor

Syngress Publishing, Inc., the author(s), and any person or firm involved in the writing, editing, or production (collectively "Makers") of this book ("the Work") do not guarantee or warrant the results to be obtained from the Work.

There is no guarantee of any kind, expressed or implied, regarding the Work or its contents. The Work is sold AS IS and WITHOUT WARRANTY. You may have other legal rights, which vary from state to state.

In no event will Makers be liable to you for damages, including any loss of profits, lost savings, or other incidental or consequential damages arising out from the Work or its contents. Because some states do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation may not apply to you.

You should always use reasonable care, including backup and other appropriate precautions, when working with computers, networks, data, and files.

KEY	**SERIAL NUMBER**
001	PK9EV4NV43
002	TQMM7T6CVF
003	8J9H4NDREA
004	ZMATTNH89Y
005	U8MPTST3V3
006	KA7HYC4ES6
007	G8JA5QNCAK
008	9J3NNY6RD7
009	T3QULAV6FH
010	5BVF7TNZEL

PUBLISHED BY
Syngress Publishing, Inc.
800 Hingham Street
Rockland, MA 02370

Configuring Symantec AntiVirus Enterprise Edition

Printed in the United States of America

1 2 3 4 5 6 7 8 9 0

ISBN: 1-931836-81-7

Technical Editor: Robert J. Shimonski
Acquisitions Editors: Catherine B. Nolan,
Andrew Williams

Cover Designer: Michael Kavish
Page Layout and Art by: Patricia Lupien
Copy Editor: Mike McGee
Indexer: J. Edmund Rush

Distributed by Publishers Group West in the United States and Jaguar Book Group in Canada.

Acknowledgments

We would like to acknowledge the following people for their kindness and support in making this book possible.

Karen Cross, Lance Tilford, Meaghan Cunningham, Kim Wylie, Harry Kirchner, Kevin Votel, Kent Anderson, Frida Yara, Jon Mayes, John Mesjak, Peg O'Donnell, Sandra Patterson, Betty Redmond, Roy Remer, Ron Shapiro, Patricia Kelly, Kristin Keith, Jennifer Pascal, Doug Reil, David Dahl, Janis Carpenter, and Susan Fryer of Publishers Group West for sharing their incredible marketing experience and expertise.

The incredibly hard working team at Elsevier Science, including Jonathan Bunkell, AnnHelen Lindeholm, Duncan Enright, David Burton, Rosanna Ramacciotti, Robert Fairbrother, Miguel Sanchez, Klaus Beran, and Rosie Moss for making certain that our vision remains worldwide in scope.

David Buckland, Wendi Wong, Daniel Loh, Marie Chieng, Lucy Chong, Leslie Lim, Audrey Gan, and Joseph Chan of STP Distributors for the enthusiasm with which they receive our books.

Kwon Sung June at Acorn Publishing for his support.

Jackie Gross, Gayle Voycey, Alexia Penny, Anik Robitaille, Craig Siddall, Darlene Morrow, Iolanda Miller, Jane Mackay, and Marie Skelly at Jackie Gross & Associates for all their help and enthusiasm representing our product in Canada.

Lois Fraser, Connie McMenemy, Shannon Russell, and the rest of the great folks at Jaguar Book Group for their help with distribution of Syngress books in Canada.
David Scott, Tricia Wilden, Marilla Burgess, Annette Scott, Geoff Ebbs, Hedley Partis, Bec Lowe, and Mark Langley of Woodslane for distributing our books throughout Australia, New Zealand, Papua New Guinea, Fiji Tonga, Solomon Islands, and the Cook Islands.

Winston Lim of Global Publishing for his help and support with distribution of Syngress books in the Philippines.

A special thanks to Robert J. Shimonski for his continuing help and dedication to so many Syngress titles.

Contributors

James Stanger (Ph.D., Symantec Technology Architect, Convergence Technology Professional, CIW Master Administrator, MCP, Linux+, A+) is co-author of Syngress Publishing's *E-mail Virus Protection Handbook* (ISBN: 1-928994-23-7) and *Hack Proofing Linux: A Guide to Open Source Security* (ISBN: 1-928994-34-2). A network security consultant and writer, James' specialties include virus management, mail server administration, intrusion detection, and network auditing. Currently Senior Course Director for ProsoftTraining, James consults with Symantec to enable security professionals to deploy virus protection, vulnerability management, and firewall/VPN solutions in enterprise networks. James has also consulted for companies and organizations such as IBM, Securify, Brigham Young University, ITM Technology, and the William Blake Archive. James is the Chairperson of the Linux Professional Institute (LPI) Advisory Council and sits on the CompTIA Linux+ and Server+ cornerstone committees. In addition to authoring books for Syngress, James has also authored security books and courses for Sybex, Osborne/McGraw-Hill, and ComputerPREP. James resides in Washington.

Chris Mosby (Symantec Product Specialist) is a Senior Network Specialist at Bechtel Hanford, Inc. He currently manages the System Management Server and Virus Protection systems for the Environmental Restoration Contract at the United States Department of Energy's Hanford Nuclear Reservation. At the time of this writing, Chris' implementation of Symantec AntiVirus Corporate Edition, and the use of other antivirus methods, has allowed his company to have zero network downtime due to virus infection, since January of 2000. He was also awarded a Gold Award Certificate by Bechtel Hanford, Inc. for his efforts during the Nimda virus outbreak, where it was calculated that the company was saved one million dollars in potential lost work. Chris is also a columnist for the myITforum.com Web site, where he has written articles on Systems Management Server and antivirus topics. Chris holds an associate's degree in Physics, and lives in Kennewick, WA with his wife, Debbie.

Athar A. Khan (Symantec Product Specialist NAVCE, MCSE, MCSA,CCA) is a Wintel (Windows Systems on Intel Platforms) Systems Engineer at a high tech company in southern California. Athar solely architected, implemented and supported a global, enterprise-wide Norton AntiVirus Corporate Edition solution using 10 NAVCE servers for 4,000+ systems in over 30 office locations and numerous home offices. As the NAVCE Administrator, Athar devised incident response strategies to prevent, contain, and counter virus threats and outbreaks including Nimda and Code Red. Currently, Athar is architecting, implementing, and supporting an enterprise-wide data backup and disaster recovery solution that will ultimately protect over 10 Terabytes of data using Connected TLM software. In addition to these responsibilities, Athar performs advanced technical support and Windows domain administration with a scope of responsibility that encompasses 500+ servers and 3,500+ clients in over 60 locations worldwide. Athar holds a bachelor's degree in Electrical Engineering from the Illinois Institute of Technology.

Scott Dentler (CISSP, CCSE, CCSA, MCSE, CCNA) is an IT consultant who has served with companies such as Sprint and H&R Block, giving him exposure to large enterprise networks. Scott's background includes a broad range of IT facets, including Cisco routers and switches, Microsoft NT/2000, Check Point firewalls and VPNs, Red Hat Linux, network analysis and enhancement, network design and architecture, and network IP allocation and addressing. He has also prepared risk assessments and used that information to prepare business continuity and disaster recovery plans for knowledge-based systems. Scott is a contributor to *Snort 2.0 Intrusion Detection* (Syngress Publishing, ISBN: 1-931836-74-4).

Jay Cee Taylor (CNA/CNE-4.11, CNA/CNE-5.0, CNA/CNE-6.0, CNS, MCP) is the Senior Network Administrator for Thomson Industries, a branch of the Danaher Corporation's Motion Group. Danaher is a leading industrial company, which designs, manufactures, and markets innovative products. Thomson is a leading manufacturer and provider of linear motion products and engineering. Jay Cee currently supports a large Novell NetWare and Windows environment, managing enterprise-wide accounts, file systems, backup solutions, and virus protection. His specialties include Novell/Microsoft administration, design, implementation, upgrades and migrations, Computer Associate's ARCserve/BrightStor products, and Symantec's NAVCE. Jay Cee has successfully performed a migration to NAVCE 7.6, and he will soon begin a NetWare 6.0 upgrade and a full migration to SAVCE 8.0. Jay Cee is a Licensed Technical Instructor who worked for several years as a Senior Instructor and Training Coordinator for Computer Career Center of Garden City, NY teaching NetWare administration and engineering, and Windows-based courses. Jay Cee is a member of NUI and currently resides in Hempstead, NY with his two best friends: his younger brother, Peter Schork, and his fiancée, Jennifer Caffiero.

Laura E. Hunter (MCSE, MCT, MCDBA, MCP, MCP+I, CCNA, A+, Network+, iNet+, CNE-4, CNE-5) is a Senior IT Specialist with the University of Pennsylvania, where she provides network planning, implementation and troubleshooting services for various business units and schools within the University. Her specialties include Microsoft Windows NT/2000 design and implementation, troubleshooting, and security topics. As an "MCSE Early Achiever" on Windows 2000, Laura was one of the first in the country to renew her Microsoft credentials under the Windows 2000 certification structure. Laura's previous experience includes a position as the Director of Computer Services for the Salvation Army and as the LAN Administrator for a medical supply firm. She also operates as an independent consultant for small businesses in the Philadelphia metropolitan area and is a regular contributor to the TechTarget family of Web sites. Laura holds a bachelor's degree from the University of Pennsylvania and is a member of the Network of Women in Computer Technology, the Information Systems Security Association, and InfraGard, a cooperative undertaking between the United States Government and other participants dedicated to increasing the security of United States critical infrastructures.

Jason E. Genser (MCP, A+) is a computer consultant specializing in systems management, antivirus and software deployment solutions, and technologies for small- and medium-sized businesses. Jason has more than ten years of extensive hands-on experience with personal computers and networks and has designed and implemented the infrastructure of a multisite, Microsoft SMS 2.0 environment for a subsidiary of Cingular Wireless. Jason is a columnist on www.myitforum.com, a leading Web site for IT professionals and system administrators. He is the technical editor of *TCP/IP Unleashed, Second Edition*, *Microsoft Windows 2000 Professional Unleashed*, and *Microsoft Windows 2000 Server Unleashed*. He is also a contributing author and editor on *Peter Norton's Complete Guide to Windows 2000 Server*. A native and life-long resident of central New Jersey, Jason is a member of the Internet Society and the North American Association of Technology Professionals.

Technical Editor and Contributor

Robert J. Shimonski (TruSecure TICSA, Cisco CCDP, CCNP, Symantec SPS, NAI Sniffer SCP, Nortel NNCSS, Microsoft MCSE, MCP+I, Novell Master CNE, CIP, CIBS, IWA CWP, DCSE, Prosoft MCIW, SANS.org GSEC, GCIH, CompTIA Server+, Network+, Inet+, A+, e-Biz+, Security+, HTI+) is a Lead Network and Security Engineer for the leading manufacturing company, Danaher Corporation. At Danaher, Robert is responsible for leading the IT department within his division into implementing new technologies, standardization, upgrades, migrations, high-end project planning, and designing infrastructure architecture. Robert is also part of the corporate security team responsible for setting guidelines and policy for the entire corporation worldwide. In his role as a Lead Network Engineer, Robert has designed, migrated, and implemented very large scale Cisco and Nortel based networks.

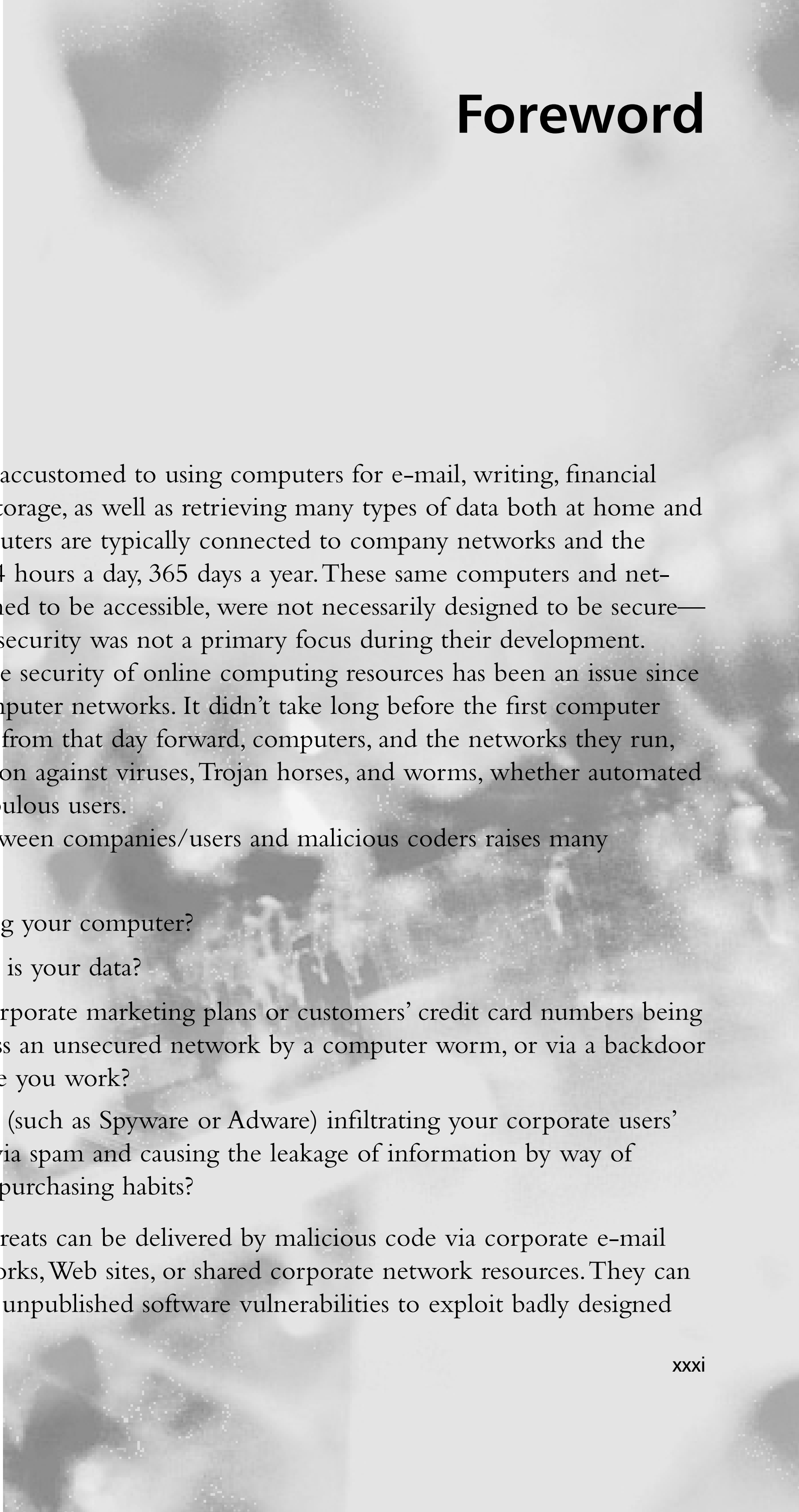
Robert has held positions as a Network Architect for Cendant Information Technology and worked on accounts ranging from the IRS, to AVIS Rent a Car, and was part of the team that rebuilt the entire Avis worldwide network infrastructure to include the Core, and all remote locations. Robert maintains a role as a part time technical trainer at a local computer school to deliver classes on networking and systems administration whenever possible.

Robert is also a part-time author who has worked on over 20 book projects as an author and editor. He has written and edited books on a plethora of topics with a strong emphasis on network security. Robert has designed and worked on some brand new topics for Syngress Publishing to include the only book dedicated to the Sniffer Pro protocol analyzer. Robert has worked on the following Syngress Publishing titles: *Security+ Study Guide & DVD Training System* (ISBN: 1-931836-72-8); *Sniffer Pro Network Optimization & Troubleshooting Handbook* (ISBN: 1-931836-57-4); *Configuring and Troubleshooting Windows XP Professional* (ISBN: 1-928994-80-6); *BizTalk Server 2000 Developer's Guide for .NET*

(ISBN: 1-928994-40-7); *SSCP Study Guide & DVD Training System* (ISBN: 1-931836-80-9); *Nokia Network Security Solutions Handbook* (ISBN: 1-931836-70-1); and *MCSE Implementing and Administering Security in a Windows 2000 Network Study Guide & DVD Training System* (ISBN: 1-931836-84-1). Robert is also a contributor to the forthcoming *Building DMZs for Enterprise Networks* (ISBN: 1-931836-88-4) and *MCSA/MCSE Exam 70-292 Study Guide & DVD Training System: Managing and Maintaining a Windows Server 2003 Environment for an MCSA Certified on Windows 2000* (ISBN: 1-932266-56-9).

Robert's specialties include network infrastructure design with the Cisco product line, systems engineering with Windows 2000/2003 Server, NetWare 6, Red Hat Linux and Apple OSX. Robert's true love is in network security design and management utilizing products from the Nokia, Cisco, and Check Point arsenal. Robert is also an advocate of Network Management and loves to 'sniff' networks with Sniffer-based technologies. When not doing something with computer related technology, Robert enjoys spending time with Erika and snowboarding wherever the snow may fall and stick.

Contents



Foreword

We have all become accustomed to using computers for e-mail, writing, financial modeling, and data storage, as well as retrieving many types of data both at home and at work. These computers are typically connected to company networks and the Internet, normally 24 hours a day, 365 days a year. These same computers and networks, though designed to be accessible, were not necessarily designed to be secure—in other words, data security was not a primary focus during their development.

Unfortunately, the security of online computing resources has been an issue since the early days of computer networks. It didn't take long before the first computer worm appeared, and from that day forward, computers, and the networks they run, have needed protection against viruses, Trojan horses, and worms, whether automated or driven by unscrupulous users.

This struggle between companies/users and malicious coders raises many concerns, such as:

- Who is using your computer?
- How secure is your data?
- Are your corporate marketing plans or customers' credit card numbers being copied across an unsecured network by a computer worm, or via a backdoor Trojan while you work?
- Is Greyware (such as Spyware or Adware) infiltrating your corporate users' computers via spam and causing the leakage of information by way of surfing and purchasing habits?

Many of these threats can be delivered by malicious code via corporate e-mail systems, public networks, Web sites, or shared corporate network resources. They can use either known or unpublished software vulnerabilities to exploit badly designed software, all for the purpose of gaining control of a user's computer. However, with all of the advancements in user education, antivirus software, and information security in general, we are still a long way from the trusted and secure computing services currently on the drawing board.

The aforementioned problems are just some of the privacy and data security issues malicious code is connected with. A sound security policy encompassing software solutions, security policies, and employee work practices is essential in effectively combating these types of threats. But, as you likely know, relying on individual computer users to protect their own computers simply does not work.

Antivirus software has been helping users protect themselves against malicious code since the first worms and viruses appeared on desktop computers in the late 80s and early 90s. Many vendors in the antivirus software industry have come and gone in the fight against viruses. Over the years, the Symantec Corporation has acquired several smaller antivirus and data security vendors for their unique technologies, culminating in the acquisition of IBM and Intel's antivirus business in the latter part of the 1990s. Both of these acquisitions were to have a significant impact on Symantec's approach to its enterprise software solutions; resulting in the birth of Norton AntiVirus Corporate Edition (NAVCE).

NAVCE breathed new life into Norton AntiVirus, and the consumer and enterprise editions headed in different directions to satisfy two distinct needs: those of the average home user, and those of the corporate network administrator. The technologies acquired from Intel and IBM—enterprise antivirus software management and automated virus handling, respectively—were the keystones of this divergence. There are, however, several common components shared by the home and enterprise products, including the core virus scanning engine and the interfaces to the Digital Immune System (DIS), where new viruses are processed and updated virus definitions are created and distributed.

These key components, along with comprehensive network management features, are the backbone of an effective enterprise antivirus software solution, and differentiate NAVCE in a highly competitive marketplace. NAVCE 7.6 gives network administrators control over the client side of the antivirus scanning product, enabling planned and controlled rollouts of product upgrades and virus definition updates.

Clients can be locked down so users cannot turn off the antivirus protection or alter the settings of the antivirus software. PC administrators can run regularly scheduled virus scans to supplement on-access scanning, and view virus activity on their client base using centralized reporting and quarantine tools.

NAVCE continues to evolve with Symantec AntiVirus Corporate Edition (SAVCE) versions 8, 8.1, and 8.5, offering additional functionality that provides comprehensive virus protection for workstations and network servers enterprise wide

Version 8.5 not only improves the speed of virus scanning as well as the delivery speed of virus definitions to workstations, but also reduces the size of these updates, and adds digital signatures to them. All this with an enhanced protection of configuration settings which offers such valuable features as the ability to re-enable real-time virus protection. It also provides improved manageability and deployment while simultaneously requiring fewer servers.

These are all improvements on the tried and tested NAVCE 7.6, which *Configuring Symantec AntiVirus Enterprise Edition* teaches you how to implement, upgrade, and configure in a diverse network environment. The authors of *Configuring Symantec AntiVirus Enterprise Edition* have experience implementing and managing NAVCE installations in enterprises that range from 50 to 5000 users with multiple servers, and have hands-on experience with the day-to-day operation of NAVCE, from installation to troubleshooting to infection recovery.

Whether you are managing an existing NAVCE 7.6 configuration or implementing SAVCE version 8.*x*, this book will help you get the most out of your software installation, allowing you to maximize your virus protection while minimizing both the cost of ownership and your own workload.

—David Banes
Symantec Security Response
Asia Pacific Regional Manager

Chapter 1

Introduction To Norton AntiVirus Corporate Edition (NAVCE)

Solutions in this chapter:

- A Brief History of Computer Viruses
- Fighting Back with Antivirus Programs
- Antivirus Solutions and the Enterprise
- Centralizing Antivirus Management
- Introducing Symantec Security Response
- Symantec Support for Operating Systems and Networks
- Symantec AntiVirus Corporate Edition 8.0
- Symantec Product Specialist Certification Information

☑ Summary

☑ Solutions Fast Track

☑ Frequently Asked Questions

Introduction

At some time in the last 15 years many of us blinked, and upon opening our eyes we found the world on the verge of becoming one large network. Public and private networks were interconnected both far and near, and now in your corner of this interconnected puzzle, virus protection for the network has become your responsibility.

With numerous unforeseeable viruses attempting to infiltrate your network, providing reliable and secure virus protection should be one of your top concerns. Norton AntiVirus Corporate Edition 7.6 (NAVCE) propels the terms "reliable" and "secure" to an exceedingly higher level. NAVCE can help protect your network, both servers and clients alike, with the most up-to-date protection in a completely automated environment.

With a well-designed and implemented deployment of NAVCE, worrying about virus protection for your network will be history. NAVCE provides a truly proactive approach to your virus protection needs that won't leave you scrambling for answers when a virus threat arises.

Understanding computer viruses, and what they are capable of, can provide you with a clearer understanding of why a product such as NAVCE should be introduced into your network structure.

NOTE

This book is intended to introduce you to the NAVCE 7.*x* AntiVirus software. It will provide you with the finer particulars to help you utilize the software to proactively *and* reactively guard your network from virus threats. Additionally, this book provides information necessary for you to pass the Symantec Product Specialist certification Exam 250-011.

A Brief History of Computer Viruses

As computers became more popular in the home and workplace, viruses followed them in through the door. Viruses are nothing more than moderately small programs designed to disrupt and alter the functionality of a computer.

The word *malicious* is defined by Merriam-Webster's Collegiate Dictionary as: *given to, marked by, or arising from malice.* Additionally, *malice* is defined as: *The desire* *to cause pain, injury, or distress to another—or—the intent to commit an unlawful act or cause harm without legal justification or excuse.* There are thousands of viruses floating around the networks of the world, and a great percentage of them fall into this definition.

However, not all viruses are malicious, some are just disruptive. Others, however, are not only disruptive, but destructive at heart, designed to destroy the recipient's system.

Malware

Malware comes from the phrase "*mal*icious soft*ware*." The term is functional in covering an entire scope of aggressive software such as Trojan horses and worms. Though malware's definition may vary, it basically describes any software or code that is specifically designed to damage and/or disrupt a system. The overall problem with this generic definition boils down to a simple issue: how one receives the malware, and whether the sender's intensions were malicious.

Hypothetically, in order to better understand malware, let's say we have constructed a secure networked lab environment so we can write, test, and study such programs. In our excitement of breaking a code we have been studying and reinventing a specific malware program, we send our findings along with the program itself to all of our co-authors*, and forget to add an appropriate subject line to the e-mail warning the recipients of the e-mail's content*. Surely, our intent was to share our findings with our peers, and not to cause any destruction to their systems. However, upon opening the e-mail and watching their entire system being formatted before their eyes, others might not perceive the issue in the same manner as we did. The program itself was purely malicious, but our intent was not. Does that make it malware? What if we had clearly warned the recipients of the e-mail's attachment and they chose to open it in an unsecured environment? Is it *then* considered malware? This is a very tricky question, with no clear-cut answer.

No matter how you perceive the generic definition offered in the previous paragraph, it is fair to say that most viruses—worms, Trojan horses, and macro viruses alike—are malware.

Viruses

For viruses to efficiently perform the devious functions their creators intend, they somehow need to be executed. Once executed, most viruses will attempt to replicate themselves throughout the computer and ultimately (if interconnected to other computers) onto the network. Viruses are activated when an infected program is loaded into memory and executed either by its own code or by the