WHITE PAPER: BEST PRACTICES SERIES FOR HEALTHCARE

Confidence in a connected world.

Critical Infrastructure Security for Healthcare Providers

White Paper: Best Practices Series for Healthcare

Critical Infrastructure Security for Healthcare Providers

Contents

Executive summary

The Best Practices Series for Health Care discusses the challenges that healthcare providers face in information technology—and the best practices for meeting those challenges. This paper, in particular, focuses on critical infrastructure security.

Practices and services implemented by healthcare providers today that improve quality of care, decrease costs, and retain top talent also foster a distributed business environment. Such practices include providing access to physicians 24 hours a day, 7 days a week; enabling new methods of communication between providers, payers, pharmacies, and patients; and working with off-premises services providers, such as transcription services and interpretation services for radiology digital imaging.

The requirements for a secure enterprise architecture are changing with the increasing interconnection between hospitals and clinics, physician remote offices, remote contractors, suppliers, university networks, and other external parties. For example, unmanaged endpoints, including laptops and mobile devices inside and outside the hospital as well as medical devices that run on common IT platforms, are proliferating. As a result, security perimeters must expand beyond the internal network to numerous critical endpoints. In this constantly evolving environment, traditional security measures, such as firewalls, antivirus, and intrusion detection systems/intrusion prevention systems, no longer provide the required granularity, protection, and enforcement.

Healthcare organizations also must comply with multiple standards and regulations regarding patient data privacy, including those issued by the Joint Commission, the Health Insurance Portability and Accountability Act (HIPAA), and individual states. Accordingly, they are implementing methods to monitor and report access to critical systems and information. In addition, they recognize the need to create and enforce security policies to protect critical endpoints, such as databases containing sensitive data, like protected health information (PHI), as well as electronic medical records (EMRs), and electronic health records (EHRs).

This white paper describes a multifaceted approach to critical infrastructure security for healthcare providers. The foundation of this approach is a comprehensive and automated enterprise security plan. As part of this plan, recommended best practices include performing comprehensive vulnerability and risk assessments; securing endpoints with proactive protection; monitoring and enforcing security on managed and unmanaged endpoints; and minimizing data leakage by securing data at rest, in motion, and in use via USB-connected devices, CDs, email, laptops, mobile devices with large memory cards, and other devices.

Characteristics of the changing healthcare environment

Today's rapidly changing operations are enhancing the quality of patient care and patient safety, yet they are also introducing security challenges due to:

- Distributed business environments
- Stringent data privacy requirements
- Constantly evolving threat landscapes

Distributed business environment

A distributed business environment can enhance provider competitiveness by providing access to systems and information to those who need it, where they need it, when they need it. Yet the demands of this environment pose some of the most significant security challenges. Today's hospital IT networks often interconnect with other networks. For example, medical centers that are associated with universities often connect their IT networks to those of the university. The security policies of these two entities, however, can differ significantly. While universities typically grant access to a broad range of users (for example, students, faculty, and staff members) without onerous security requirements, healthcare providers must enforce much stricter policies to ensure patient privacy and comply with various regulations.

The distributed business environment extends to a range of other users within the network as well (see Figure 1). In addition to interconnections between departments (such as radiology, oncology, administration, laboratories, pharmacies, and others), secure access is needed for remote clinics, physicians' offices, regional health exchanges, and insurance companies. Remote access applies to individuals such as physicians working from home, home visiting nurses, patients, and others. A variety of contractors, such as transcriptionists, IT service providers, medical imaging interpretation services, partners, and suppliers, also require access. These individuals access the networks via laptop computers and mobile and handheld devices.

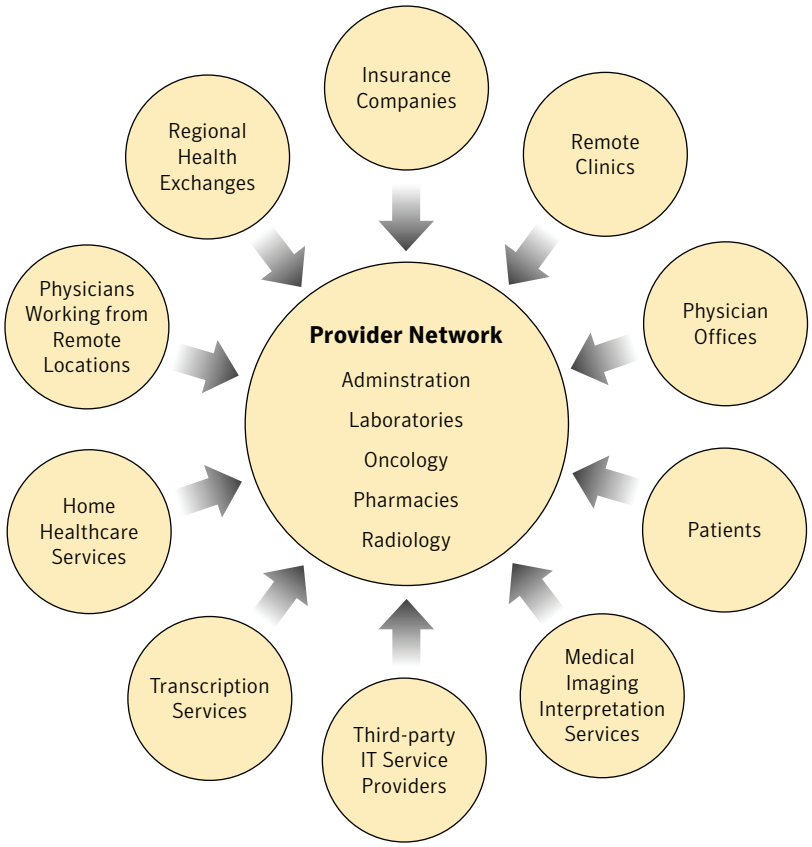

Figure 1. The distributed business environment in healthcare presents a range of security challenges.

According to one source, approximately 150 people have access to patient records during a typical hospitalization.[1] Given the explosion of users accessing provider networks, in many cases, access control is not sufficiently policy driven, up to date, or thorough. In addition, paper-based records and other information are susceptible to information leakage from photocopying and offsite archiving.

[1] "At risk of exposure: In the push for electronic medical records, concern is growing about how well privacy can be safeguarded," *Los Angeles Times*, June, 26, 2006, http://www.latimes.com/features/health/medicine/la-he-privacy26jun26,1,3180537.column?ctrack=1&cset=true

Data privacy

HIPAA regulations, Joint Commission accreditation, and state privacy and other regulations mandate patient data privacy. Databases, for example, need to be secured, while maintaining appropriate and legitimate access, including treatment, payment, and operations (TPO), as well as reporting and auditing. In everyday practice, maintaining such data privacy is not easy. In one recent example, an online billing company inadvertently exposed protected health information (PHI) on about 9,000 people after turning off a firewall to perform maintenance. The PHI included the names, addresses, birth dates, and Social Security numbers of patients of a major healthcare provider in the northeastern United States. After the firewall error exposed the information, Google catalogued the stored information, making it temporarily available on Google.com. Implicated in other breaches, the billing company subsequently went out of business.[2, 3] This example illustrates the ineffectiveness of the traditional security model (for example, a perimeter firewall and security measures on hosts).

Healthcare providers face conflicts not encountered in other industries. For example, medical devices cannot be patched quickly or security measures added easily due to the need to comply with FDA requirements. At the same time, providers must protect networks and systems that are critical to the continuity of core hospital functions. Furthermore, ease of access for physicians and nurses (to protect human health) often takes a higher priority than stringent security. Security measures cannot be overly prohibitive or complicate access to systems; otherwise, they will not be acceptable. They also need to allow authorized users (such as a network administrator) access for monitoring and reporting.

Evolving threat landscape

In the midst of this ever-changing business and regulatory environment, the threat landscape is evolving. Critical threats include data breaches that could lead to identity theft, threats to confidential information, malicious code such as Trojan horses, and others. These threats can not only compromise patient and provider data, but also reduce the reliability and/or availability of IT systems—systems that are critical in life and death situations.

Identity theft is an increasingly pressing issue, particularly for organizations that store and manage such information. Compromises that result in the loss of personal data can be costly, not only to the people whose identity may be at risk and their respective financial institutions, but

[2] "Billing Company blamed in breach," *Concord Monitor*, June 11, 2007, http://www.concordmonitor.com/apps/pbcs.dll/article?AID=/20070611/REPOSITORY/706110383/1043/NEWS01
[3] "Medical IT Contractor Folds After Breaches," Tim Wilson, *Dark Reading*, August 15, 2007, http://www.darkreading.com/document.asp?doc_id=131712&WT.svl=news1_1

also to the organization responsible for collecting the data. In the first half of 2007, the education sector (which includes research hospitals) accounted for more data breaches that could lead to identity theft than any other sector (30 percent of the total). This statistic is particularly relevant due to the interconnection of many university networks with provider networks.[4]

Some malicious code programs are designed specifically to expose confidential information that is stored on an infected computer. These threats expose sensitive data such as system information, confidential files and documents, or logon credentials and can lead to significant data leakage. Some of the primary malicious code threats that appeared in the first half of 2007, such as backdoors, can give a remote attacker complete control over a compromised computer. Keystroke loggers, which record keystrokes on a compromised computer and relay them to a cybercriminal, were another primary type of malicious code threat to confidential information in the first half of 2007.[4]

These two types of threats are merely examples of those that inhabit the current landscape. Additional prominent threats include phishing (as a means of identity theft), Trojan horses (typical of multistage attacks), bot-infected computers, and others. And the healthcare industry, like others, has experienced significant data breaches. For example, in July 2006, a contractor helping a Midwest provider with medical billing records exchanged a bag containing CDs with medical and billing records of 260,000 patients. (The bag was subsequently returned to the hospital.)[5] Then, in September 2006, hackers broke into a database of an Ohio hospital, gaining access to the medical records of up to 230,000 patients.[6] For ongoing information about emerging threats, organizations can refer to Symantec's Internet Security Threat Report, which offers an analysis and a discussion of recent threat activity. Published twice yearly, the report covers Internet attacks, vulnerabilities, malicious code, phishing, spam, and security risks as well as future trends.[7]

Healthcare automation

Picture archiving and communication systems (PACS) and other digital medical imaging systems; bedside IP-based devices; and EMR, PHR, and EHR systems all improve access to healthcare information, quality of care, and patient safety as well as reduce costs. The trend in automating healthcare delivery services is accelerating investment in information technology, with benefits being accrued by both patients and providers. Yet accompanying those benefits is the responsibility to secure records and the databases in which they reside. Automation measures deliver greater

[4] "Symantec *Internet Security Threat Report*, Trends for January-June 07," Volume XII, September 2007, http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xii_09_2007.en-us.pdf
[5] "Perot Systems Walks Off With Indiana Hospital's Patient Data," Martin H. Bosworth, ConsumerAffairs.Com, http://www.consumeraffairs.com/news04/2006/10/st_francis_data.html
[6] "Hackers Attack Ohio Children's Hospital Records," Martin H. Bosworth, ConsumerAffairs.Com, http://www.consumeraffairs.com/news04/2006/10/akron_hospital_data.html
[7] *Internet Security Threat Report*, www.symantec.com/business/theme.jsp?themeid=threatreport

interconnection and pave the way for adoption of state-of-the-art technologies, such as service-oriented architecture. These technologies, in turn, introduce new security and privacy challenges. Many IT departments are working with their business unit partners and security vendors to design and implement security and privacy measures prior to project deployment to decrease the costs associated with implementing security as an afterthought.

Security best practices for healthcare providers

A comprehensive enterprise security plan begins with the creation of a roadmap that includes best practices such as:

- Performing comprehensive risk assessments
- Identifying critical endpoints based on criticality of uptime, importance to business processes, and susceptibility to a security or privacy incident
- Defining cost-effective measures to secure critical endpoints, including mobile devices and databases, and minimizing data leakage
- Implementing automation for ongoing measurement of existing security effectiveness, adherence to security policies, and regulatory compliance
- Implementing automation for monitoring, quickly identifying and responding to policy violations, and reporting on security and privacy on multiple levels—from executive dashboards to detailed reports for IT staff

Perform risk assessments

Security best practices begin with risk assessment (also known as vulnerability assessment). A 2007 healthcare security survey stated that the area in greatest need of improvement in security is risk assessment. Yet, about two-thirds of providers do not conduct risk assessments, and less than one-half ensure that security policies include risk assessment.[8, 9]

Achieving a balance between healthcare network access and security is challenging. By applying risk management approaches, providers can achieve the appropriate balance at a reasonable cost. Such an assessment addresses people and processes, in addition to technology.

[8] "Information Security Still an Issue in Health Care," Vance Cariaga, *Investor's Business Daily*, September 7, 2007, http://www.accountability-central.com/single-view-default/single-view-lexis-nexis/browse/2/article/information-security-still-an-issue-in-health-care/?tx_ttnews%5BbackPid%5D=113&cHash=279ef33347&type=123

[9] "The Global State of Information Security 2007," PriceWaterhouseCoopers, 2007, http://www.pwc.com/extweb/pwcpublications.nsf/docid/114E0DE67DE6965385257341005AED7B/$FILE/PwC_GISS2007.pdf

Both electronic and paper (hard copy) vulnerabilities should be examined. And healthcare CIOs need benchmarks, such as the identification of specific areas that involve security and an indication of how well the average organization is addressing each area.

Risk assessments include an evaluation of network vulnerabilities, including security of the perimeter, endpoints, and internal network. IT professionals typically perform penetration testing on these networks as well as outward-facing applications. They evaluate policies and procedures across a wide range of activities (practices for providing secure billing and many others). Physical security assessments (such as physical entry security and paper security practices) complement cybersecurity assessments.

Secure endpoints

A second critical area is protection of network endpoints—desktops, laptops, mobile devices, databases, and various types of servers. This includes granular security for usage of memory cards, USB-connected devices, CDs, and DVDs. Many new, sophisticated threats can evade traditional security solutions, leaving organizations vulnerable to data theft and manipulation, disruption of critical services, and damage to brand and reputation. To stay ahead of this emerging breed of stealthy and resilient security threats, providers need to advance their endpoint protection.

One important aspect of this protection is the need to be proactive. Antivirus, antispyware, and other signature-based protection measures, which are primarily reactive, may have been sufficient to protect an organization's vital resources a few years ago, but that is not the case today. Best practices now employ proactive endpoint security measures that can protect against zero-day attacks (attacks that exploit vulnerabilities before patches or updates become available) and even unknown threats.

Since there are a variety of threats and vectors of attacks and incidents, endpoint protection involves more than one type of security mechanism. While protecting all devices with the same level of security is typically not financially viable, critical devices need to be armed with antivirus, antispyware, desktop firewall, intrusion prevention, and device control technology. However, deploying these security products individually on each endpoint is not only time-consuming, but it also increases IT complexity and costs. Organizations then need to provide management, training, and support for a variety of different endpoint security solutions. Also, differing technologies often work against one another or impede system performance because of high resource consumption.

To reduce the complexities and costs associated with deploying and managing multiple solutions, Symantec recommends that the solutions be consolidated into a single, integrated agent that can be deployed and administered from a single, unified management console. A single endpoint security agent enables operational efficiencies such as a single communication method and content delivery system across all security technologies. Service configuration and exclusions can be performed globally at one point on the client or at the management server. Furthermore, automated security updates to the agent provide hassle-free protection from the latest threats.

To ensure that threats cannot take advantage of vulnerabilities resulting from the way a device is configured, providers need to ensure that all endpoints—including onsite employee, remote employee, and guest endpoints—that attempt to connect to the network are configured according to the organization's security policies. An end-to-end network access control (NAC) solution helps ensure that all endpoints are in total compliance with such policies before they can access the network and its resources, or only a minimal set of resources such as a connection to the Internet (see Figure 2). Similar to a "sandbox" approach, this solution is particularly important when unmanaged endpoints (computers and devices not under the direct control of the provider) attempt to access the network. It should also seamlessly integrate with existing network infrastructures and be simple to deploy and manage.

In the past, security experts have debated over whether firewalls need to be placed only on the perimeter of an organization's network or on individual desktops as well. The current threat landscape and the extended computing infrastructures of organizations with a mobile workforce have made endpoints a primary target for exploits and attacks. A threat often first infects a single laptop while outside the network perimeter, and then when the laptop connects to the internal network, it spreads to other endpoints. Endpoint firewalls can be used not only to block internal network attacks from breaching any endpoint connected to the network, but also to prevent these threats from ever leaving the initially infected endpoint.

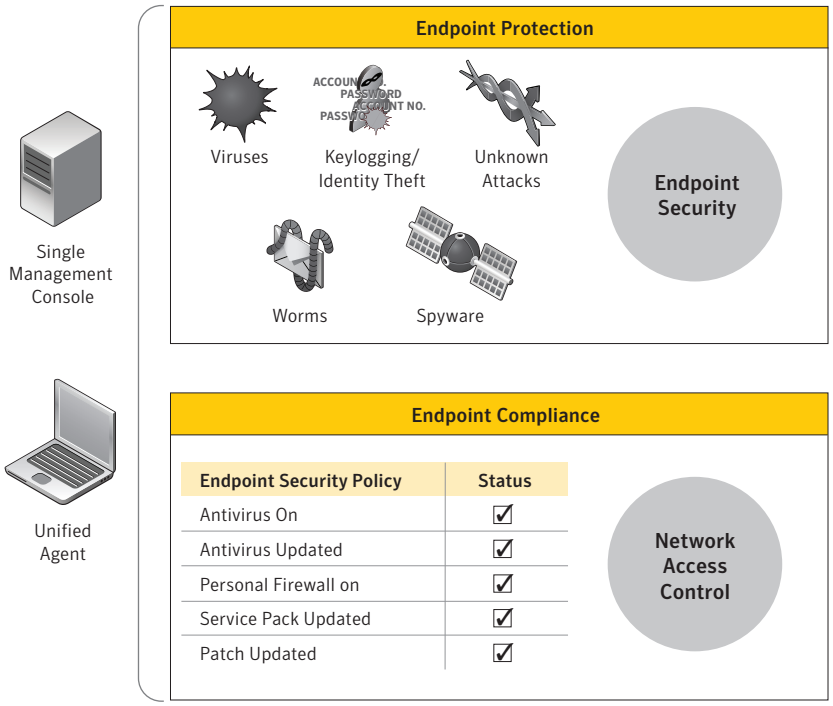

Figure 2. Recommended approach to endpoint security.

Symantec solution boosts network and data health

Touchstone Behavioral Health of Glendale, Arizona, provides evidence-based behavioral treatment programs for at-risk children. This provider sought a solution to secure its network against malware acquired by laptops used in field work, protect against network intrusions and malware from user downloads, and maximize security and data protection services with a small IT staff. Touchstone adopted a Symantec solution and approach that integrated a variety of protection technologies in one product, allowing centralized management. According to Steven Porter, IT director at Touchstone, "There's money being made in penetration, in hacks and viruses, in spam, so the threats that we chase are constantly evolving. To combat that with a single product and a single console makes it a little bit easier." To date, the solution has already quarantined laptops on nine occasions before they could contaminate the network.

Minimize data leakage

Data loss or leakage has become a major security problem for healthcare providers. Most of this data leakage is due to flawed business practices or lack of compliance with company policies. Many provider CIOs recently interviewed by Symantec have had to take disciplinary action against employees, including doctors, for unauthorized access to records. Examples include doctors who access the records of family members, and hospital workers who access the records of a person with whom they have social contact. Such insider threats also include inattentive, complacent, or untrained employees; dissatisfied or disgruntled employees; demoted or terminated employees; or an employee motivated by financial gain.[10] Particularly disturbing is the abuse of network access by administrators, who can also cover their tracks.

[10] "Insider Security Threats: State CIOs Take Action Now," NASCIO, 2007, http://www.nascio.org/publications/documents/NASCIO-InsiderSecurityThreats.pdf

Symantec recommends a three-pronged strategy for minimizing data leakage:

- Secure and encrypt data at rest
- Secure and encrypt data in movement between nodes
- Secure data in use

Securing data at rest (that is, secure databases) involves database auditing (for example, maintaining an audit trail of all SQL activity), database fraud detection (for example, by using fraud policies and historical transaction information), and database leakage detection. Key solution components include intruder identification, heuristic learning (via real-time, ongoing monitoring, cleanup, and recommendations of acceptable behavior), and establishment of transaction policies. According to provider CIOs recently interviewed, data in motion presents a major concern, namely, the loss of data via USB-connected devices. This area is difficult to secure due to the myriad legitimate uses of such devices.

Implement mobile security

Today's mobile devices contain a vast amount of sensitive and confidential information. Devices such as PDAs and Windows® based smartphones represent the new computing platform, one that providers are increasingly adopting. For instance, Symantec research indicates that an overwhelming majority of enterprises allow corporate data on devices but do not address smartphone security. Meanwhile, nearly as many enterprises report security as their greatest mobility obstacle. With so much sensitive data residing on mobile devices, the threat of loss or theft poses serious risks. And with loss and theft rates spiraling upwards, particularly for phones, organizations are exposed to data disclosure on multiple levels.

The increasing prevalence of these devices also makes them vulnerable to new attack vectors that are more damaging and discreet than previous threats. For example, the latest attack vectors include "snoopware" and "pranking4profit." Snoopware is a Symantec-coined term for mobile spyware that remotely places a phone into diagnostic mode and then activates the microphone to monitor conversations. Pranking4profit attacks access premium mobile SMS payments, resulting in theft.

Best practices begin with the development and deployment of centrally defined mobile device security policies. Mobile device management (MDM) systems enable administrators to conduct centralized device monitoring and administration via a management console. They roll out installation packages, send down new configurations, collect log events, and conduct loss mitigation techniques such as "wipe and kill" to protect any proprietary information on lost or stolen phones. Teaming these capabilities with classic security measures such as antivirus protection, firewalls, antispam functionality, network access control, and tamper protection helps harden security perimeters at these vulnerable endpoints.

Promote regulatory compliance, policy enforcement, and centralized monitoring

Healthcare providers need to interpret regulations and standards; map controls to them to automate compliance measurement, reporting, and enforcement; set new business and IT policies; and modify existing policies. This process involves, for example, setting policies to minimize threats identified in the risk assessment process, as well as establishing procedures for controlling damage in case of security incidents. In the healthcare industry, policies must be clear and complete; some provider CIOs state that misunderstandings about policies are common.

Centralized information management is an important practice not only to enhance data protection, but also to help authorized users, such as network administrators, monitor, audit, and report. It also enables the adoption of managed security services. A centralized, managed security solution, for example, would have detected the disabled firewall in the example described in "Data privacy." A database-access monitoring tool would also most likely have detected suspicious activity during this incident and raised a flag. An integrated security agent deployed on the database would then have dropped the connection, preventing this incident from occurring. Centralized management also assists forensic analysis—determining what happened and who is responsible—and security log management.

Symantec portfolio of security solutions for healthcare providers

The table lists some critical infrastructure challenges that healthcare providers face and corresponding Symantec solutions.

Challenge	Symantec Solution
Performing vulnerability/risk assessments	Symantec™ Global Intelligence Services
Securing endpoints, including desktops, laptops, servers, and mobile devices, network access control	Symantec™ Endpoint Protection
Minimizing data leakage and/or loss from insider threats and faulty business processes	Symantec Database Security Symantec Endpoint Protection Symantec™ Control Compliance Suite
Centralizing security information reporting and management	Symantec™ Security Information Manager Managed Security Services
Protecting against new attack vectors that use mobile devices	Symantec™ Mobile Security
Protecting against viruses and spam for email and instant messaging	Symantec™ Mail Security 8300 Series
Automating security policy creation, monitoring, reporting and automating IT compliance processes	Symantec Control Compliance Suite
Enforcing behavior-based security processes	Symantec™ Critical System Protection

Conclusion

Symantec recommends the following best practices for healthcare providers:

- Apply risk management approaches to achieve the appropriate balance between access and security at a reasonable cost; examine both electronic/cyber and paper vulnerabilities.
- Protect endpoints (such as desktops, laptops, mobile devices, databases, and various types of servers) with proactive measures via a single integrated agent; ensure that each endpoint complies with security policies before accessing the network; include endpoint firewalls in the solution.
- Minimize data leakage by securing/encrypting data at rest via database auditing, fraud detection, and leakage detection; secure/encrypt data in motion between nodes; and secure data in use.

- Develop and deploy centrally managed mobile device security policies, including technologies such as MDM systems that protect against snoopware, pranking4profit, and other mobile threats; implement MDM systems that roll out installation packages, send down new configurations, collect log events, and “wipe and kill” lost/stolen phones.
- Interpret regulations and standards; map controls to them to automate compliance measurement, reporting, and enforcement; set new business and IT security policies; and modify existing policies.
- Centralize information management to help authorized users effectively monitor, audit, report, and conduct forensic analysis, as well as to adopt managed security services, if so desired.

About Symantec

Symantec is a global leader in infrastructure software, enabling businesses and consumers to have confidence in a connected world. The company helps customers protect their infrastructure, information, and interactions by delivering software and services that address risks to security, availability, compliance, and performance. Headquartered in Cupertino, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free 1 (800) 745 6054.

Symantec Corporation
World Headquarters
20330 Stevens Creek Boulevard
Cupertino, CA 95014 USA
+1 (408) 517 8000
1 (800) 721 3934
www.symantec.com

Printed in the U.S.A. 11/07 13535672