



Securing Your Data Against Today's Threats, and Tomorrow's Unknown Breakthroughs

Prepared for EMBARQ by Guideline, Inc.

May 2008

Security
Whitepaper

A Dangerous World: Increased Use, Increased Risk

As more businesses rely on their data network systems to communicate within and among their offices, with off-site staff, and with vendors and customers, they are more vulnerable to the accidental, purposeful, machine-made, or man-made mishaps that can damage the integrity of their proprietary information.

- *Forty-four percent of network professionals serving small-to-medium sized businesses reported having a network device go down for at least one hour during work hours during the past year. In addition, thirty-seven percent reported having the primary network server go down for at least an hour.*
- *Remote monitoring services were found to significantly reduce network downtime. The average network-down incident was nearly fifty percent shorter when the affected device/server was covered by a remote monitoring managed service.*
- *The average end-user reported that network downtime reduces their work productivity between forty-nine percent and sixty-nine percent, depending on the length of downtime. Responses also varied significantly by industry and job role.ⁱ*
- *Estimates reveal that losses through employee abuse through email may cost companies as much as \$50 billion per year.ⁱⁱ*

The list of bad things that can happen to a company's data network system is not endless, but certainly long enough to generate a palpitation or two. Network systems can be attacked by viruses, worms, and Trojans, or hacked by industrial spies. Laptops with vital information can be lost or stolen. Access to a website on the Internet can open the door to spyware, spam, phishing and pharming attacks.

- *Furthermore, the list is constantly changing and growing as hackers and developers of malware - the various types of software intended to do harm to computers and networks - continue to proliferate.*
- *It is possible that the threat that will be the most common a year from now has not even been conceived of today.*
- *This constantly evolving, ever more dangerous environment, requires IT managers to have more and better resources available to them for dealing with the changing nature of the threats.*

While many of these dangers are associated with home computers, the increasing use of office computers for workers' personal business has opened the door to these threats attacking a company's network.

- *In addition, the growing prevalence of telecommuting, in which employees work from their homes - and home computers - through remote access to their companies' networks, has also opened the door to viruses and other malicious software.*

But even businesses that do not allow these practices are still highly vulnerable. This is particularly so for businesses which have valuable data transmitted over their network, such as identity-related information (such as social security numbers), credit card numbers, intellectual property, customer lists, engineering plans, etc.

The results of these attacks, intrusions and accidents in companies' networks may include the loss of business continuity, reduced employee productivity, lower revenues and weak customer goodwill. The danger these threats pose cannot be underestimated. A business that chooses to ignore them might as well post a "Going out of Business" sign.

The pace and volume of malware initiatives makes it imperative that businesses be proactive in their security efforts in order to stay ahead of the malware curve.

Threats to Data Networks: The Enemies List

THREAT	DESCRIPTION
Computer Viruses	<p>Programs that infect files on a data network system or a file system that another computer may access. By replicating themselves in these files, viruses enter computers without the permission or knowledge of their users until they have thoroughly penetrated and infected the data network system.</p> <ul style="list-style-type: none"> • <i>Malignant viruses are designed to damage programs and make them inoperable.</i> • <i>Benign viruses do not harm computers. Instead they launch messages, eat up memory and contribute to system crashes.</i>
Computer Worms	<p>Self-replicating programs that use data networks to send copies from one computer to all the others in the network. Worms are different than viruses in that they can operate on their own and do not have to attach themselves to an existing program or file.</p> <ul style="list-style-type: none"> • <i>Worms harm data network systems by consuming large amounts of bandwidth and by slowing down all other programs.</i>
Trojan Horse	<p>A software program that is supposed to perform one task but instead is a cover for a program that does something completely different. That other program can be a worm or a vehicle for a virus.</p> <ul style="list-style-type: none"> • <i>A Trojan horse may also be a decoding program that allows a hacker to access data that would otherwise be off limits.</i>
Hackers	<p>Computer experts who use their skills to gain unauthorized access to a data network system. Some hackers are randomly destructive, doing harm because they find an opportunity.</p> <ul style="list-style-type: none"> • <i>Hackers may also be industrial spies, targeting a specific company whose proprietary information they have been charged with stealing or destroying.</i>
Spyware	<p>Programs that typically infiltrate a data network through an Internet connection without the user's knowledge, for the purpose of gathering information contained in that network.</p> <ul style="list-style-type: none"> • <i>Spyware may also insert itself into the network or an individual computer on the network to change settings, redirect activities and undermine protections in the system, opening access for viruses that would have been blocked otherwise.</i>
Phishing	<p>The effort to fraudulently acquire proprietary information, such as usernames, passwords and credit card details, by using a false identity in an electronic communication.</p> <ul style="list-style-type: none"> • <i>Phishers typically represent themselves as representatives of well-known companies, organizations, or government agencies.</i>
Pharming	<p>Refers to the activity of hackers that redirect a website's traffic to another website.</p> <ul style="list-style-type: none"> • <i>Internet users think they are forwarding information or funds to one site when in fact they are forwarding the information to another site that has been set up in order to steal from the real site.</i>

Source: Guideline, Inc. 2008

Threats Increase as Networks Expand

As businesses' data networks expand to include remote components, the number of potential threats they face increase. The Internet Security Alliance (ISA) has noted that:

“Attackers are constantly bombarding components accessible from the Internet with query functions looking for weaknesses. Unprotected devices are compromised within minutes after connectivity is established especially when Internet access is available through cable modems, digital subscriber lines, or other high-speed connections. A compromised device puts all other devices on the network at risk since it can be used as an inside base for locating weaknesses and attacking other components on the network.”ⁱⁱⁱ

The ISA has also noted that growing use of wireless access:

- *Point-of-sales devices and inventory devices communicate to central servers via wireless.*
- *The ability to reach and use services on a network from outside (called remote access) is extremely valuable for traveling employees, suppliers, and customers.*
- *Remote access also allows technology vendors to provide support for critical network services quickly without having to travel to your site.*
- *Employees can and do add remote access devices directly to their computer so they can work from offsite.*

Use of wireless access to a business's network demands careful control. Industry observers have noted that the spread of Web 2.0 technology and increased traffic to social-networking sites on business computers has made remote and mobile devices the preferred points of attack for hackers and malware disseminators.

- *Instant messaging, chat sessions and music-sharing capabilities establish peer-to-peer routes into the network, bypassing many of the traditional network security mechanisms.*
- *These options are a growing conduit of malicious code and must be used carefully.*

Financial Impact of Security Breaches

In “2007 Malware Report: The Economic Impact of Viruses, Spyware, Adware, Botnets, and Other Malicious Codes” the research firm [Computer Economics, Inc.](#) estimated that the value of direct damages from malware worldwide was \$13.3 billion in 2006.

The report also notes that this figure was a decrease from the \$14.2 billion in damages incurred in 2005 and the 2004 \$17.5 billion figure.

Financial Impact of Malware Attacks 1997-2006

Worldwide Impact (U.S. \$)	
2006	\$13.3 Billion
2005	14.2 Billion
2004	17.5 Billion
2003	13.0 Billion
2002	11.1 Billion
2001	13.2 Billion
2000	17.1 Billion
1999	13.0 Billion
1998	6.1 Billion
1997	3.3 Billion

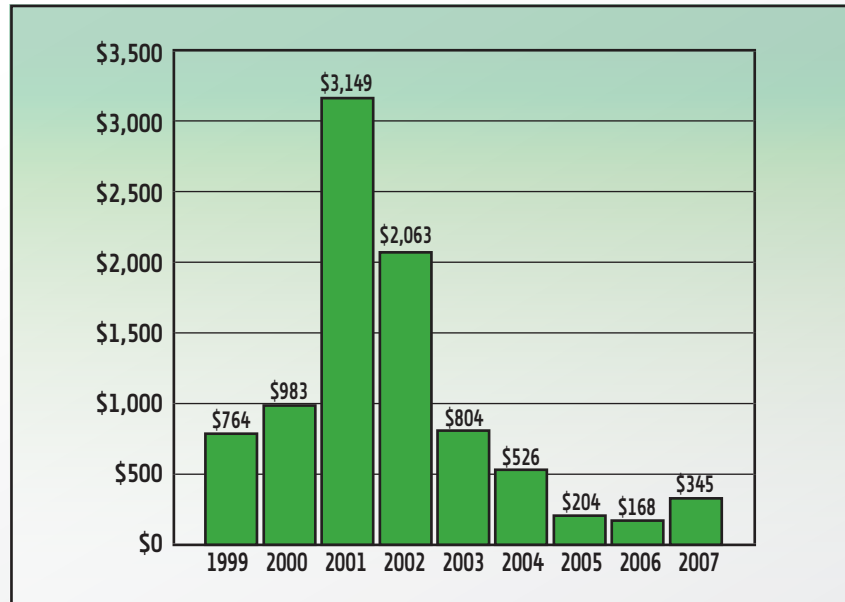
Source: Computer Economics, 2007,
Used by permission. All rights reserved.

Figure 1

According to [Computer Economics](#), there are two key factors that have contributed to the decline of financial losses related to direct damage from malware.

- *On the positive side, most enterprises have beefed up their use of anti-virus protection systems that manage to keep pace with developments on the malware side.*
- *On the negative side, the drop in direct damage may be more than made up in losses further down the road as malware authors focus on stealing from enterprises rather than merely causing chaos.^{iv}*

Average Loss per Respondent (in \$ 000)



Source: "The 12th Annual Computer Crime and Security Survey," *Computer Security Institute*, 2007

The breaches cited included:

- *insider abuse of Internet access or email*
- *laptop or mobile device theft*
- *system penetration by outsider*
- *viruses, worms and spyware*

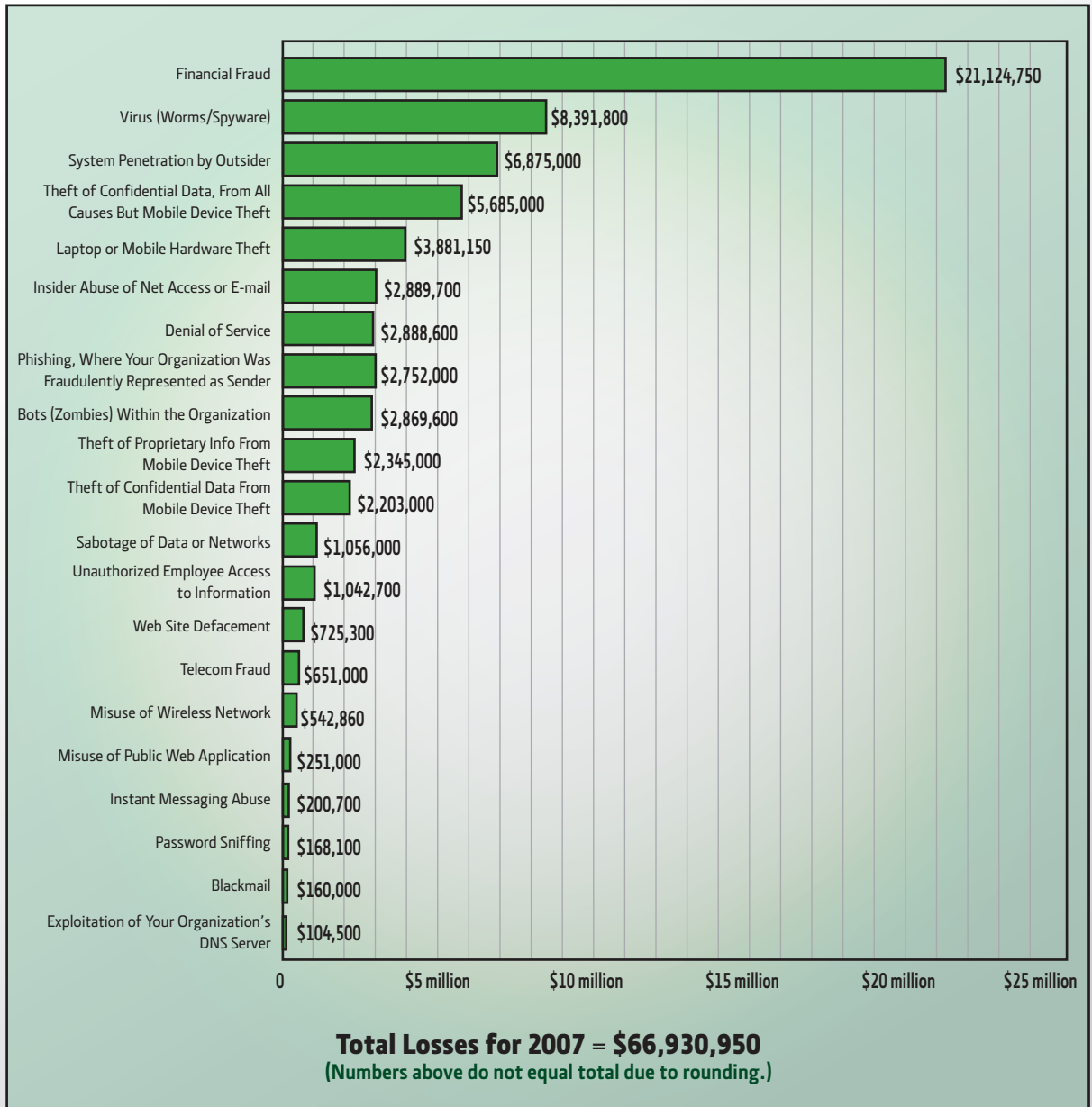
Data network outages from security breaches also contribute to a considerable amount of lost productivity. A recent survey of IT professionals by the Computing Technology Industry Association (CompTIA) uncovered the following information on spyware infections:

- *More than one in four end-users reported having their productivity impacted by a spyware infection during just the prior six months. Of those, more than one-third reported getting multiple infections.*
- *The average infected user reported "living with" their spyware problem for eighteen work hours before getting it repaired.*
- *The average infected user reported that his or her spyware infection reduced his or her work productivity between twenty-one percent and thirty-two percent. However, these figures varied significantly by industry and job role.^v*

Respondents to the Computer Security Institute's "12th Annual Computer Crime and Security Survey" reported an average loss of \$345,005 as a result of some type of security breach. The 2007 figure was higher than the previous two years' figures, but well below the average losses reported by respondents in 2001 and 2002.

- Financial fraud was the cause of the largest amount of loss, followed by viruses/worms/spyware and then penetration by outsiders, or hackers.
- In general, the significant drop reflects enterprises' aggressive adoption of security measures after enduring major security breaches.^{vi}

Dollar Amount Losses Among Respondents by Type of Attack



Source: "The 12th Annual Computer Crime and Security Survey," Computer Security Institute, 2007

Enterprises of All Sizes at Risk

Large enterprises represent a good target for security attacks because, given their size, they offer so many points of vulnerability. According to Computer Economics' "2007 Malware Report: the Economic Impact of Viruses, Spyware, Adware, Botnets and Other Malicious Codes," at the median, organizations experience five malware events per year. This figure rises to ten events per year for organizations with over five thousand desktop computers.

- *The economic impact of malware events increases as organizational size increases.*
- *Based on the level of implemented defenses, the impact of malware events varies widely between organizations.*

But, as the Internet Security Alliance points out, small and medium-size enterprises are hardly in the clear:

"Many small and medium-size businesses are under the mistaken impression that their size, or the minimal security steps that they have already taken, will protect them from cyber attacks. This assumption is both inaccurate and dangerous. Attacks on information systems operated by small and midsize companies are growing rapidly and are having a severe impact on business operations. One survey showed that about one out of every three small businesses was affected by the recent [2004] "MyDoom" virus twice the proportion of large enterprises that were hit by the same virus."^{vii}

The Impact of "Self-Created" Losses

EMPLOYEES BEHAVING INAPPROPRIATELY...

While outside sources such as spyware and hackers create serious problems for data network systems, enterprises' own employees may also add to the problem. Over the last few years, an important part of many firms' data network security systems now includes controls on employee use of the Internet.

Among the inappropriate activities employees engage in at work are:

- *accessing pornography*
- *gaming*
- *instant messaging*
- *investing*
- *shopping*
- *watching videos or listening to music*

Some observers have noted that thirty to forty percent of all Internet use in the workplace is not related to business and that nearly two of every three employees use workplace Internet access for their personal affairs during business hours.

- *Nearly two out of every three companies in America has disciplined an employee for inappropriate use of the Internet. In addition, nearly one in three companies has terminated an employee for such behavior.*
- *The first online Victoria's Secret fashion show in 2000 reportedly cost corporate America more than \$120 million in productivity in just forty-four minutes.*

Cognizant that these abuses occur, many businesses try to curtail employees' ability to check e-mail and/or make phone calls. Nevertheless, estimates reveal that losses through employee abuse may cost companies as much as \$50 billion per year. This figure includes losses related to law suits resulting from employees' use of email or the Internet for unlawful activity.

Furthermore, when employees access pornography or gaming websites, they may allow malware to access their companies' data network systems, leading to losses that dwarf the lost productivity of that idling worker.

... OR MAKING MISINFORMED MISTAKES

Apart from the damage that employees can do to data networks by using the Internet for personal reasons, they may cause network damage through carelessness and neglect. No matter how good the passwords and security controls on a computer, laptop, or PDA are, an employee may unknowingly circumvent the company's established security system. According to the ISA:

"Cleaning and maintenance staff, visitors and employee family members can download malicious code or accidentally change and destroy files and programs while using the computers. Locking the device to a table or wall is not sufficient protection for the data and software stored on it."^{viii}

The ISA recommends the following precautions to prevent employee mistakes:

- *Electronic devices should not be left unattended inside or outside the office, especially while a user has an account logged on and active.*
- *If network access plugs are active in open areas such as empty offices, conference rooms and reception areas, outsiders can plug in a device to compromise the network.*
- *Anyone with physical access to a firm's electronic device, including repairmen, technical support and family members, can bypass installed controls and see, change and destroy data and programs on your computer.*
- *If your device is connected to the network, the data and programs on other computers on the network are also at risk.*

Liability Takes a Toll

A company whose data network is breached by an outsider must incur financial losses from fraud or theft; the cost of repairing the damage, and the indirect costs in terms of lost productivity. To further add insult to injury, another layer of cost includes fines for failing to protect confidential employee or customer data.

Legislative initiatives introduced during the past decade, such as the Sarbanes-Oxley Act (SOX), the Gramm-Leach-Bliley Act (GLBA), and the Health Insurance Portability and Accountability Act (HIPAA), generally target corporate and criminal fraud by company insiders.

Under Sarbanes-Oxley, it is a crime to destroy, alter, or falsify records with penalties that can include fines, imprisonment, or both.

- *There is no direct reference to computer security in Sarbanes-Oxley, which is largely focused on the accuracy of financial reporting data. IT security is important under Sarbanes-Oxley only to the extent that it supports the reliability and integrity of financial reporting.*
- *However, some interpreters of the law have suggested that a failure of data network security to prevent or detect fraud may make a company liable for the resulting losses.^{ix}*

The Gramm-Leach-Bliley Act (GLBA), also known as the Gramm-Leach-Bliley Financial Services Modernization Act, opened up competition among banks, securities companies and insurance companies and allowed commercial and investment banks to consolidate. In exchange for creating new opportunities for financial institutions, GLBA also includes a Safeguards Rule which requires these institutions to design, implement and maintain safeguards to protect customer information.

- *The Rule applies not only to financial institutions that collect information from their own customers, but also to any companies, such as credit reporting agencies, that receive customer information from financial institutions.*
- *Violation of GLBA may lead to penalties up to \$100,000 for companies and up to \$10,000 for individual officers and directors for each such violation.^x*

Under HIPAA, enterprises are liable if they have not been vigilant in preventing network security breaches that expose personal employee or patient information to unauthorized viewers.

- *Title II of HIPAA, the Administrative Simplification (AS) provisions, establishes national standards for electronic health care transactions and national identifiers for providers, health insurance plans and employers.*
- *The AS provisions also address the security and privacy of health data. The standards are meant to improve the efficiency and effectiveness of the nation's health care system by encouraging the widespread use of electronic data interchange.*
- *The Enforcement Rule sets civil money penalties for violating HIPAA rules.^{xi}*

In addition to Sarbanes-Oxley, GLBA and HIPAA, businesses that process credit card payments need to be compliant with the Payment Card Industry Data Security Standard (PCI DSS). The Standard was developed by the major credit card companies as a guideline to help organizations that process card payments prevent credit card fraud, cracking and other security vulnerabilities and threats.^{xii}

- *A company that processes, stores, or transmits payment card data must be PCI DSS compliant or risk losing its ability to process credit card payments and may be audited and/or fined.*

A Focused Response: Security from Your Network Manager

MONITORING MAKES A DIFFERENCE

While monitoring a system cannot ward off every attack, most industry observers believe that it is easier for an enterprise to get back on track if its data network system is monitored. According to research by CompTIA, for example, user downtime and repair time for monitored devices is significantly lower than for unmonitored devices.^{xiii}

Time Lost: Monitored vs. Unmonitored Network

SYSTEM STATUS	DOWNTIME IN HOURS	REPAIR TIME IN HOURS
Monitored Network	3.1	5.5
Unmonitored Network	6.0	10.4

Source: Guideline, based on "Making the Case for Managed Services," *Computing Technology Industry Association (CompTIA) and Kotler Marketing Group.*

SECURITY ACROSS ALL NETWORK LAYERS

The ISA notes that while enterprises reference their technology environments as “networks,” it is important to remember that in reality they are collections of individual devices assembled in a certain way to meet the technology-specific needs of an organization. Therefore the lesson to take away is that all components, including those on site, those in remote locations and, increasingly, mobile devices, must be protected.

“Good network security requires access protection for each component on the network including firewalls, routers, switches and all connected user devices. Otherwise, anyone who could reach your network could locate and compromise network components and services. In addition, remote and portable devices should be required to authenticate themselves to the network to limit who can see and access the network services such as databases, shared files and printers.”^{xiv}

Even as individual components are protected, there still remains the need to protect networks as a whole. Security for Local Area Networks (LAN) and Wide Area Networks (WAN) should include network-wide measures such as:

- *threat controls*
- *network admission control*
- *identity-based controls*
- *traffic visibility services*
- *malware containment services*

In addition, there is a growing focus on protections that are more inward- rather than outward-looking, with the focus on data leakage prevention (DLP). Also known as anti-data leakage or data loss prevention, the goal of DLP is to inspect content as it moves across the network set up barriers that keep data contained within the LAN or WAN, rather than focusing on keeping out external threats.

Your Data Network Manager as Security Provider: Knowledge, Partnership, Reputation

Faced with so many challenges and from so many directions, enterprises are faced with a choice between diversifying their security efforts among a variety of products and services; trying to match each threat with a different defense; or focusing efforts through a single, comprehensive security provider that can monitor the data network systems.

Industry observers consistently agree that a single provider is the best way to go and that your network system manager is in the best position to be that single provider.

One of the strengths of our portfolio, as mentioned below, is that the local or in house IT can off load some of the responsibility and resources associated with monitoring these ever changing, ever increasing threat levels.

There are three key reasons why you should use your data network manager as the source of your network security: knowledge, partnership and reputation.

KNOWLEDGE

Your data network manager already knows your system inside and out and is, as a result, in the best position to implement multi-function network security across all layers of your network (desktop, mobile, LAN, WAN, etc.) without compromising network performance or manageability.

- *In addition, your data network provider is not just aware of the network's functionality, but is also familiar with your enterprise's business goals. As a result, your system manager is in a position to anticipate where your system will be expanding and where future danger spots may turn up.*

PARTNERSHIP

Providers are already working closely with your enterprise's IT administrators and are well-positioned to take a proactive role in providing network control and access to reduce security lapses.

- *Working together in the management of the system, and its growth and expansion, your data network manager and IT department can also coordinate efforts to thwart potential attacks on the system by anticipating potential points of vulnerability.*

REPUTATION

Your concern about the security of your data network focuses on issues of financial loss, lost productivity and the possibility of liability if data is stolen from your system are all extremely serious concerns. Added to that is the loss of reputation you suffer as a business that can be trusted.

- *In this last concern, your data network manager has an equal share if it is responsible for the security of that system. A data network manager that invites the opportunity to provide security is telling you that it is not afraid to put its reputation on the line.*

Your data network manager can be a partner dedicated to the security of your system and as determined as you are to ensuring that your business stays in business.

Endnotes

- i “Making the Case for Managed Services,” *Computing Technology Industry Association (CompTIA) and Kotler Marketing Group*.
- ii “Common Sense Guide to Cyber Security for Small Businesses,” *Carnegie Mellon University and Internet Security Alliance*. All rights reserved.
- iii “Common Sense Guide to Cyber Security for Small Businesses,” *Carnegie Mellon University and Internet Security Alliance*. All rights reserved.
- iv “2007 Malware Report: the Economic Impact of Viruses, Spyware, Adware, Botnets, and Other Malicious Codes”, *Computer Economics, Inc.*
- v “Making the Case for Managed Services,” *Computing Technology Industry Association (CompTIA) and Kotler Marketing Group*.
- vi “The 12th Annual Computer Crime and Security Survey,” *Computer Security Institute* (2007).
- vii “Common Sense Guide to Cyber Security for Small Businesses,” *Carnegie Mellon University and Internet Security Alliance*. All rights reserved.
- viii “Common Sense Guide to Cyber Security for Small Businesses,” *Carnegie Mellon University and Internet Security Alliance*. All rights reserved.
- ix <http://www.sec.gov/spotlight/sarbanes-oxley.htm>
- x <http://banking.senate.gov/conf/>
- xi <http://www.hhs.gov/ocr/privacysummary.pdf>
- xii <https://www.pcisecuritystandards.org/>
- xiii “Making the Case for Managed Services,” *Computing Technology Industry Association (CompTIA) and Kotler Marketing Group*.
- xiv “Making the Case for Managed Services,” *Computing Technology Industry Association (CompTIA) and Kotler Marketing Group*.



EMBARQ[®]
BUSINESS

© 2009 Embarq Holdings Company LLC. All rights reserved.
The name EMBARQ and the jet logo are trademarks of Embarq Holdings Company LLC.

Corporate Headquarters:
5454 W. 110th Street
Overland Park, KS 66211

Telephone:
877-4EMBARQ

Website:
embarq.com
embarq.com/securitywhitepaper