



SECURING A
BUSINESS:
What Small and Medium
Sized Businesses (SMB's)
Need to Know

A Frost & Sullivan White Paper
Sponsored by Cisco Systems

Author: Jarad Carleton, Senior
Consultant, ICT Practice

TABLE OF CONTENTS

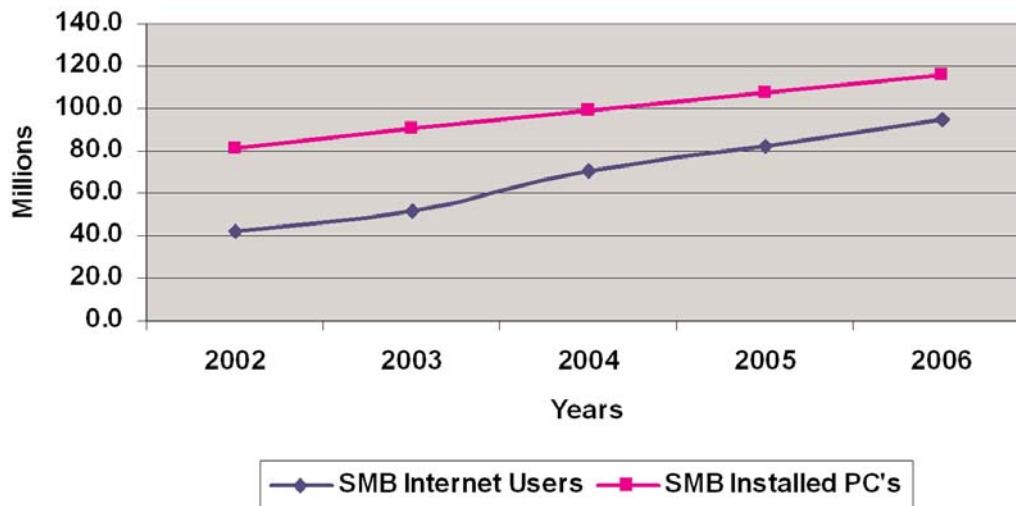
TABLE OF CONTENTS

Securing a Business – What SMB's Need to Know	3
Challenges & Issues to Securing Your Business	4
Threat Control	4
Business Availability	5
Secure Communications	6
Protecting Customer Satisfaction and Your Brand	6
The Frost & Sullivan Viewpoint on Securing Business	8
Conclusions	9
Appendix – The SMB Network Security Checklist	10

SECURING A BUSINESS – WHAT SMB’S NEED TO KNOW

As a business tool, the Internet has done more for small- and medium-sized business (SMB) flexibility, productivity, and customer service than the telephone, the post office, fax machines, and professional printing services combined. This fact is supported by the worldwide increase in SMB computer use and Internet connectivity between 2002 and 2006.

Global SMB Computer and Internet Use (2002-2006)



Source: Frost & Sullivan, Decision Support Database

In short, the Internet has given SMB's a necessary boost to easily reach out to customers large and small, domestically and internationally. It has also been responsible for enormous growth in digital information that was previously stored on paper-based records or computer systems that were not connected to the Internet.

Unfortunately, these advantages allow business-critical applications and data to be accessible on the Web, resulting in network security drawbacks. It is vital that SMB's understand these drawbacks in order to ensure the continued safe and reliable use of the Internet as a business tool.

Data Theft vs. IP Theft

Data theft and IP theft are frequently confused with each other although they describe different types of electronic content acquisition that is criminal in nature.

Data theft usually describes the criminal acquisition of records such as credit card numbers, driver's license numbers, passwords, or bank account numbers.

IP theft refers to the criminal acquisition of intellectual property material that is copyrighted, patented, or considered to be a trade secret such as blueprints or software code.

Network security issues that SMB's should be educated about and prepared for include terms that are now common for businesses of all sizes. These include:

- Spam
- Viruses
- Trojan Horses
- Worms
- Distributed Denial of Service (DDoS) attacks
- Data theft
- Intellectual Property (IP) theft
- Phishing and Spear Phishing

These terms are now understood by an increasing number of business people without IT expertise, which is a clear indicator that SMB's are beginning to realize that securing their business is necessary and that the challenge cannot be ignored.

Complicating matters further, some forward-thinking businesses have moved beyond email and instant messaging (IM) as the primary communication tools that leverage the network. These progressive companies are implementing Voice over Internet Protocol (VoIP) technologies to transport voice communications over networks and enable the use of unified communications platforms. As a result, email, IM, voice mail, telephone calls, call forwarding, and presence indicators can be combined to simplify communication with employees, partners, and customers regardless of location.

Integrating multiple applications with the company network and the Internet is extremely useful for competitive-minded SMB's. However, the result of leveraging networks for so many uses also means that each part¹ of the network must be secured against unauthorized access to prevent theft of customer data, IP theft, loss of network resources, erosion of customer loyalty, declining revenues, and more.

CHALLENGES & ISSUES TO SECURING YOUR BUSINESS

The challenges to securing a business in today's global economy are numerous and should be addressed through constant vigilance of security vulnerabilities and continuing education of employees. Periodic vigilance and education is not an option because unsecured SMB's are more prone to data theft and loss of reputation, customers, and revenues. In short, SMB's that have not secured their business are less competitive and may not be able to survive in the face of more attentive competitors that constantly adapt to resolve new security issues. Although the challenges discussed in this paper are not an all-encompassing list, they should be viewed as an educated starting point for SMB's that are serious about securing their business.

Threat Control

Worms, viruses, Trojans, and other attacks are among the biggest problems for SMB's today. To protect networks against these and other attacks, businesses need to employ a layered security policy.² Since many SMB's do not have dedicated IT professionals to identify network security weaknesses and correct them, it is important to choose a

1. These include, but are not limited to, application servers, load-balancing equipment, network- and Web-dependent applications, networked storage, routers and others

2. Layered security includes features such as physical security (locks on the doors), network authentication (one-, two-, or three-factor authentication), VPN's, firewalls, Intrusion Prevention Systems (IPS), Antivirus (AV), content filtering, and more.

trusted IT security advisor that provides sound guidance regarding hardware and software security solutions. This approach will provide the SMB with a higher level of security. However, the business can still be vulnerable due to the time lag between security patch availability and implementation by a part-time network security advisor. This leaves a window of opportunity open for zero-day exploits³ that hackers can take advantage of.

Zero-day exploits are easily leveraged by hackers and demonstrate the challenge associated with threat control for SMB's. Unfortunately, the problem is getting worse. According to the CERT/CC,⁴ the number of vulnerabilities discovered has increased over the last six years from 1,090 in 2000 to 5,340 for the first three quarters in 2006, and the number of security breaches reported has increased exponentially. However, the challenge is not overwhelming when SMB stakeholders take the time to assess potential vulnerabilities and develop action plans to proactively address them.

Thus, each significant part of the networked SMB should be examined starting with the most critical systems such as email; instant messaging clients; Web conferencing applications; credit card databases; networked storage with sensitive customer, partner, intellectual property, or human resources records; and VoIP. The reason that SMB's have networks in place is to leverage them as a tool for productivity that lowers operational costs. However, leveraging the network for as many uses as possible will also increase the vectors of attack and put an unsecured SMB at risk of data and resource loss when the business does not remain vigilant and prepared to address new threats proactively.

Business Availability

Widespread disruption of communications networks resulting from natural disasters such as hurricanes, earthquakes, floods, or man-made disasters have forced businesses to examine the reliability of networked mission-critical hardware and software. Although a SMB may use redundant network connections to primary and secondary service providers to ensure network availability, these plans can be hampered when the organization isn't prepared to adapt to changing security challenges.

Many SMB's can't afford a day of lost business that can occur when a security threat arises. For SMB's, maintaining business availability at all times is critical to ensuring customer loyalty and continued business success. When the organization cannot maintain business availability, it risks irreparable damage to its reputation and to the trust customers place in the business.⁵

The financial losses that a SMB faces following a disaster or network attack are daunting and include the expense of having to rebuild its reputation as well as shoulder the costs of recovering lost or corrupted data and network resources. These losses can be

3. An attack that occurs immediately after a security vulnerability has been announced.

4. Computer Emergency Response Team/Coordination Center – The Software Engineering Institute of Carnegie Mellon University.

5. If data is stolen during the business disruption, the SMB could be subject to civil litigation as well as fines and remedial action from governmental agencies.

exacerbated when SMB's are dependent on electronic transactions to conduct business, and customers have come to expect business availability even in times of disaster.

Secure Communications

Secure transport of voice, data, wireless, and remote communications is an essential part of ensuring business availability and relies heavily on proactive threat control. It can also be difficult for businesses to ensure, particularly when data is handed off from one network to another as is the case with email, IM, VoIP, remote, and wireless communications.

Corporate governance initiatives for SMB's have made headway in curtailing unauthorized wireless network deployment in offices, and the encryption of wireless communications has markedly improved. However, regularly scheduled security assessments should be planned to help the business keep up-to-date with security patches. In addition, the utilization of intrusion prevention systems (IPS) for wireless networks should be seriously considered to further secure the business as a whole.

Securing email and IM technologies is particularly essential due to thousands of malicious and highly damaging worms, viruses, Trojans, and phishing campaigns. Because these mission-critical communication tools are under constant threat, the use of continuously updated AV technologies, firewalls, IPS, and content filters are essential for protecting business communications.

Among the newest and most important methods of communications that requires secure transport is VoIP. For businesses that have implemented this revolutionary communications technology, ensuring the security of voice traffic is crucial to prevent interruption of telephone service. VoIP shares similar issues with data networks regarding the need to be secured against attacks from malicious traffic. However, voice traffic is unique in that it can be affected by DDoS, which can significantly impact VoIP quality of service (QoS) before rendering other communication tools ineffective. As a result, proactive steps should be taken to secure VoIP to avoid spoofing, theft of services, eavesdropping, and other security breaches.

Without secure transport of voice, data, wireless, and remote access, it is impossible for SMB's to operate reliably, which is what customers and partners expect. Furthermore, insecure transport undermines the fundamental tenets of security including confidentiality and integrity, without which businesses of any size can become undesirable.

Protecting Customer Satisfaction and Your Brand

Good business managers know that acquiring new customers is five times as costly as satisfying and retaining your current customer base. However, the cost associated with

losing customers also multiplies over time by slowly eroding the brand equity of a business, making it easier for competitors to gain market share.

As newspapers around the world continue to report on data security breaches, one of the most important acts a company can do to protect brand equity and customer satisfaction is to protect customer data. This data includes information such as addresses, taxpayer ID numbers, driver’s license numbers, phone numbers, credit card numbers, and products or services purchased to name a few examples.

Perhaps one of the worst outcomes of a customer data breach is identity theft, which can result in financial ruin, false arrest for criminal activity, and more. In these unfortunate cases, a single customer can easily make a well publicized accusation against the company whose data breach led to criminal activity and cause irreparable harm to its brand and future revenues for years to come.

Only through compliance with clearly defined regional or global data security standards can a business protect customer satisfaction and valuable brand equity. Acknowledging the importance of securing a business is not just a U.S. phenomenon. In fact, many regions around the world are addressing network and data security issues today as shown below.

A Global Standard	Payment Card Industry (PCI) Data Security Standard – PCI has improved security in the credit card industry by setting out clear definitions and requirements for compliance and disruptive punishments for noncompliance.
European Union	Directive 2002/58/EC – the EU directive on privacy and electronic communications requires the 27 EU member states to harmonize national laws regarding data security to protect the confidentiality of communications.
Tunisia	The Data Protection Act (loi organique relative à la protection des données personnelles) – a law based on the EU data protection directive that created a government appointed Data Protection Commission assigned to enforce the law.
Mexico	Model Electronic Commerce Law – amends four previous laws to create a legal framework for ecommerce that requires businesses to encrypt data, keep customer records confidential, and establishes penalties of up to 2,500 times the prevailing minimum wage in the Federal District for noncompliance.
Australia	Privacy Act – the act established 11 privacy principles with principle 4 addressing the storage and security of personal information. The act requires businesses with access to personal information to implement measures that prevent loss, unauthorized access, modification, disclosure, or misuse of such information.
India	Information Technology Act – this law addresses issues pertaining to electronic data interchange and electronic communications. It created penalties for cyber crime, breach of confidentiality, and breach of privacy, thereby encouraging businesses to improve security for their networks and data.

Data Breaches are Common

Data breaches are more common than many consumers might think. Although consumers are becoming more aware of the threat of identity theft, data breach notification laws have made personal information loss front page news. Furthermore, credit card companies are now holding card processors financially responsible for lost data.

In a recent example in January 2007, it was revealed that the U.S.-based retail conglomerate TJX stores lost 40 million credit card numbers and an unknown number of drivers’ license numbers to hackers. Since that time, stolen cards have been used fraudulently and it has been suggested that TJX was not complying with the PCI data security standard.⁶

And it appears that TJX is not alone in noncompliance. Visa indicates that only 31% of its largest merchants comply with security standards, opening the door for millions of dollars in fines.⁷

6. Sidel, Robin. “TJX Data Breach Poses Woe for Bank.” The Wall Street Journal, 19 January 2007, C4.
7. Ibid, C4

Although the examples provided are not an all inclusive list of every data security effort around the world, it is meant to show that the issue is considered serious and is global in nature. SMB's seeking to protect the financial viability of their business need to take the issue of securing business networks seriously. Those that don't secure their business are walking an increasingly dangerous path that may expose the organization to legal liability and fines in many centers of business around the world.

THE FROST & SULLIVAN VIEWPOINT ON SECURING BUSINESS

In order to adequately tackle the challenges of securing a business, Frost & Sullivan recommends four key areas for businesses to consider when critically examining the security of the organization.

1. **Layered Architecture** – Remember that no single solution will solve all security problems. Businesses must employ multiple security layers, starting at the perimeter and moving out to the endpoint⁸ itself.
2. **Vulnerability Assessment** – Regularly scheduled vulnerability assessments are important in helping businesses look at numerous risk factors and determining which are the most critical. Regular assessments also ensure that security patches and changes are effective and have been implemented methodically across the organization without overlooking any devices connected to the network.
3. **Employee Education** – All businesses need the help of employees to secure the business. Educating employees drastically reduces the success of social engineering attacks associated with viruses, Trojans, worms, and phishing. Employee education should also explain the importance of security and help to prevent inadvertently giving away sensitive information that can be used to attack the business, for example, weak or unprotected passwords, which can seriously undermine efforts to secure the business.
4. **Disaster Recovery** – The data that resides on networked computers and storage devices is mission-critical for SMB's and must be available on demand 7 days a week. Thus, when a SMB becomes a victim of malicious code, it can be a traumatic and financially painful event. A forced work stoppage can result as the network and individual computers crash or have to be shut down to contain the security threat. The impact of an attack can continue to drag productivity and revenues down even after the threat is eliminated when it is discovered that data has been corrupted or lost. Having a well-planned disaster recovery strategy in place can ensure that recovery will be swift and guaranteed after an attack. However, the best way to avoid using a disaster recovery plan is to proactively secure your network against possible threats before disaster strikes.

8. An endpoint is a terminal (computer) or gateway that can generate or terminate an information stream.

CONCLUSIONS

Although an organization cannot guarantee 100% security for its network, it is possible to for the SMB to raise the security bar so high that criminals will look elsewhere for easier prey. When a SMB is vigilant and committed to regularly scheduled security assessments and continuing education on the topic, security breaches are much less likely. Protecting the integrity of the network so that business can continue is the top priority of SMB's today. It is also a challenge that requires a serious commitment and a sense of urgency when weaknesses are discovered.

Due to the critical nature of data and communications in today's SMB business environment, all aspects of an organization's network, ranging from internal and external access to voice and data communications, must be secured. And only by examining all potential avenues of attack and establishing a secure network foundation will a business be able to protect the authenticity and integrity of data and communications on the network.

Securing the SMB in a networked and globally interconnected marketplace is not an easy task. However, it is a challenge that can be met and successfully conquered with unwavering commitment and understanding of what is at stake for the business. Security is about business survival and only the SMB's that implement a layered security strategy will protect business revenues and the brand, while cementing customer loyalty. The choice is simple and SMB's that want to survive can no longer wait to secure their business.

APPENDIX – THE SMB NETWORK SECURITY CHECKLIST⁹

Take Inventory of Your Current Security Technologies – Do You Have the Following?

1. Firewall
2. Virtual Private Network (VPN)
3. Intrusion prevention
4. Virus protection
5. Secured wireless network
6. Anomaly detection
7. Identity management
8. Compliance validation

Identify Your Most Important Digital Assets and How They Can Be Accessed

1. What are your digital assets?
2. What are they worth?
3. Where do they reside?
4. Who has access and why?
5. Do all employees have the same level of network and application access?
6. Do you extend access to partners and customers?
7. How do you control, validate, and monitor that access?

Evaluate the Potential Impact of a Security Breach

1. What is the potential financial impact of a network outage due to a security breach?
2. Would a security breach be likely to disrupt your supply chain? How?
3. What would happen if your Web site went down?
4. How long would the site be down before you suffer a significant financial impact?
Minutes? Hours? Days?
5. Do you have ecommerce features on your site?
6. How long could your storefront be unavailable before you suffer a significant financial impact? Minutes? Hours? Days?
7. Does your company have insurance against cyber attacks or misuse of customer data?
8. Is that insurance adequate?

Consider Current and Future Needs

1. In what ways do you expect your business plan to evolve over the next few years?
2. How recently have you updated your network equipment? Software? Virus definitions?
3. What type of security training do you provide to your employees?
4. How will growth affect your digital assets and their value to your business as a whole?
5. In the future, are you likely to have a greater need for remote employees, customers, or partners to access those digital assets?

9. Martin, James A. "Technical Matters: Addressing Network Security." iQ Magazine, Vol. VI, No. 2, 72.

CONTACT US

Palo Alto

New York

San Antonio

Toronto

Buenos Aires

Sao Paulo

London

Oxford

Frankfurt

Paris

Israel

Beijing

Chennai

Kuala Lumpur

Mumbai

Shanghai

Singapore

Sydney

Tokyo

Silicon Valley
2400 Geng Road, Suite 201
Palo Alto, CA 94303
Tel 650.475.4500
Fax 650.475.1570

San Antonio
7550 West Interstate 10, Suite 400,
San Antonio, Texas 78229-5616
Tel 210.348.1000
Fax 210.348.1003

London
4, Grosvenor Gardens,
London SW1W 0DH, UK
Tel 44(0)20 7730 3438
Fax 44(0)20 7730 3343

877.GoFrost
myfrost@frost.com
<http://www.frost.com>

ABOUT FROST & SULLIVAN

Based in Palo Alto, California, Frost & Sullivan is a global leader in strategic growth consulting. This white paper is part of Frost & Sullivan's ongoing strategic research into the Information Technology industries. Frost & Sullivan regularly publishes strategic analyses of the major markets for products that encompass storage, management, and security of data. Frost & Sullivan also provides custom growth consulting to a variety of national and international companies.

The information presented in this publication is based on research and interviews conducted solely by Frost & Sullivan and therefore is subject to fluctuation. Frost & Sullivan takes no responsibility for any incorrect information supplied to us by manufacturers or end users.

This publication may not be downloaded, displayed, printed, or reproduced other than for non-commercial individual reference or private use within your organization, and thereafter it may not be recopied, reproduced or otherwise redistributed. All copyright and other proprietary notices must be retained. No license to publish, communicate, modify, commercialize or alter this document is granted. For reproduction or use of this publication beyond this limited license, permission must be sought from the publisher.

For information regarding permission, write:

Frost & Sullivan
2400 Geng Rd., Suite 201
Palo Alto, CA 94303-3331, USA