White Paper

Easy Guide to Comprehensive IT Security Strategies for SMBs

High-End Endpoint Security, Data Loss Prevention and Portable Device Management at a Reduced Scale

July 2008

COSOSYS

Table of Contents

Corporate Trends Overview

The current business environment requires high levels of competitiveness from all players in the market. Large companies need to keep working on preserving their market position while challengers and small and medium sized companies have to put up a similar effort in gaining and retaining their customers. Given these circumstances, the difference between companies is limited to size only when it comes to their resources and strategies. The complexity, adaptability and innovation for the solutions they employ need to be similar in order to maintain competitive advantages.

Innovation is the main tactical advantage SMBs have to compensate the immense marketing and financial power large companies make use of. They need to keep innovating to determine the smart paths of business that get them to the top without spending fortunes on each of their actions. Resourcefulness when it comes to innovations also means an increased risk of industrial espionage, employees being bribed or blackmailed and other tools from the dark side of business.

Emerging businesses or SMBs thus generate needs leading developers to present solutions of high end features, yet adapt them to the dimensional requirements of these companies. As they must face their competitors with matching complexity in strategy and tactics, SMBs start to re-evaluate their IT infrastructure needs and choose vendors based on more than price and licensing volume. They look for the same finesse, time saving and business advantages that their larger competitors are looking for.

When it comes to IT and security infrastructure, SMB characteristics are translated to those of the personnel involved in developing and maintaining them. Such companies have limited numbers of experts monitoring their systems and implementing new solutions, therefore prevention gains significantly more focus over repairing damages. That is why developing comprehensive and proactive security policies and determining the best fit solutions to enforce them should be a persistent concern for emerging companies.

Assessing the Risks and Finding the Right Solutions

While most businesses are aware of the classical threats, such as viruses, Trojans, phishing attacks and other kinds of malware, when it comes to implementing endpoint security and data loss prevention solutions, what is protected and against whom is harder to define. This security segment focuses on protecting and controlling endpoints from within a certain network (such as PCs or laptops) and those attached to the existing infrastructure – from thumb drives to smart phones and music players.

As employees continuously request to be IT-enabled at all times, making sure all their portable devices are protected at all times becomes a valid concern. According to a recent research performed by financial services provider Barclaycard Business and quoted by Computing.co.uk, business travelers are increasingly using technology to maximize productivity and save time on their trips. Therefore, they are making a point from asking airlines, airports and other companies in the travel industry for more technological advancements.

According to the study, some 66% of those surveyed would like airlines to provide wireless internet connections to maximize time while traveling. This opens up the door to data theft, data loss, unauthorized access to private data and much more.

Which Are the Threats and What Needs Protection?

Using portable storage devices to steal corporate information is not a new practice, yet USB Flash Drives, smart phones or portable music players continue to gain popularity, becoming common accessories, thus making it extremely easy to either carry data outside a certain enterprise or to cause serious malware infections, putting and end to most activities for hours or days.

While preventing uploads of potentially malicious files without authorization, endpoint security software also prevents information theft or loss. More importantly however is that they highlight a threat commonly overlooked: the inside threat. Most surveys and reports show insiders are those behind the majority of security breaches. Be it intended or a simple mistake, such breaches come at a high price.

The 2005 CSI/FBI computer crime and security survey shows the theft of proprietary information went up from $168,529 in 2004 to $355,552 in 2005. Moreover, according to the Computer Crime Research Center, in 2005 98% of all crimes committed against companies in the U.K. had an insider connection.

In April 2007, the Palo Alto Networks released a survey releasing troubling findings: employees in most enterprises are constantly circumventing corporate security policies by deploying unauthorized applications, including video viewers, streaming audio, P2P, and Google applications. Given this breach savvy attribute of possible employees, all gateways are open to stealing and loosing classified information.

Examples are more powerful than abstract numbers, so it would help pointing out that quite a few of the security breaches occurring in the past few months of 2008 were caused or believed to be caused by insiders. That was the case for the second largest breach ever reported occurring at Hannaford, where 4 million credit card accounts were exposed to identity theft and fraud, or for the Downingtown High School where a student stole 55,000 private records or for the Southeast Missouri State University.

How to Determine the Real Costs of Security Breaches?

Endpoint security solutions mainly focus on protecting data stored and transited through the network. Information bits, be it private records of customers and employees or intellectual property, is know to have high value, yet it is hard to quantify. But one can come to a rather accurate image of what is at stake by creating a few scenarios: think what effects the loss of a commercial software product's source would generate; or think of a new service model stolen and immediately implemented by your main competitor; alternatively, imagine what costs rebuilding your reputation would entail after exposing all your customers to identity theft by losing their social security numbers, bank accounts or usernames and passwords for online purchases through your online shop.

Given recent legal measures taken by courts or governments, the costs of loosing private data is easier to perceive. In the United States for example, in January 2006, the Federal Trade Commission charged commercial data broker ChoicePoint Inc. a settlement fee of 15 million dollars for leaking consumer data and violating consumer privacy rights (Federal Trade Commission, 2006). Also, in the first months of 2008 the state of California has passed a bill obliging companies where data breaches occur to disclose the full extent of such incidents to those affected. It is probably only a matter of time until other states and countries enforce similar harsh measures which entail high costs needed to both comply with disclosure requirements and identity management.

Lost confidential data comes with a price in the UK as well. A Ponemon Institute survey from 2008 shows that the average price a company pays for a lost private record is of £47, while the average total price paid by a company exposed to data breaches is of £1.4 million.

Is Stealing Information Difficult?

In this day and age, definitely not. With the proliferation of small yet powerful storage devices, theft is becoming quite common. In 2005, the Yankee Group reported that almost 37% of businesses surveyed held USB drives responsible for contributing to the disclosure of company information. Nearly two thirds of the leaks resulted in some disruption to the business units involved, according to the analyst firm. More recently, Symantec's Internet Security Threat Report released in early 2008 showed that stolen or lost hardware, from laptops to USB sticks and portable hard drives were the most common cause of data breaches in 2007, outranking malicious software.

Also, given the ease of catching data thieves, the process of breaching a company's security system and stealing private records is far from complicated. Earlier this year, Canada's largest telecom provider, Bell Canada, has recovered the personal data of about 3.4 million customers. The thief has been capture after being overheard when trying to randomly sell the information to several individuals.

Is Data Loss that Common?

According to most sources, it is becoming more and more common and is mainly related to portable storage devices. Symantec's Internet Security Threat Report Volume XI shows that, in 2006, theft or loss of a computer or data storage medium, such as a USB memory key, made up 54% of all identity theft-related data breaches. Symantec's report for the next year, 2007, showed that lost hardware was one of the first to causes of data breaches, along with theft.

A more recent survey performed by the Ponemon Institute and commented by Computerworld.com in June, 2008, shows some of the largest and medium-size U.S. airports report close to 637,000 laptops lost each year, most of them misplaced at checkpoints and during security checks. That's about 10,000 laptops lost at airports each week. Moreover, laptop theft is quite common in the U.S according to Mike Spinney, a spokesman for the Ponemon Institute.

In a study conducted by the institute, 76% of companies surveyed reported losing one or more laptops each year, of which 22% were due to theft or other criminal mischief.

The wide spread of hardware loss is not only common in private sector companies. An audit performed in May 2008 at the US State Department has revealed the loss of over 1,000 laptops. The timeframe for the loss was not clearly determined, nor the conditions in which the losses occurred.

Dozens of other such breaches and losses are reported every week. There are sites such as Attrition.org Data Loss Archive and Database specialized in monitoring and reporting on such events. And it happens within infrastructures that we imagine as being fully secured, such as the military.

In 2006 flash drives containing classified US military secrets turned up for sale at a marketplace in Afghanistan, Bagram. In the same year, the Dutch army lost classified data in similar circumstances not once, but twice. To further exemplify, early in 2008, a USB stick containing classified NATO information was found in a library in Sweden. The stick in question contained sensitive details on NATO's ISAF peace-keeping force in Afghanistan and an intelligence report on the attempted assassination targeting Lebanon's defense minister and the murder of Sri Lanka's foreign minister.

Standard Compliance – Added Value of Endpoint Security

Endpoint security is regarded as a rather new niche of the IT security field. Yet its importance in overall wellbeing of both customers and companies is recognized by both laws and debated standards. Complying with international standards such as HIPAA, Sarbanes-Oxley, PCI or GLBA, as well as with country specific data breach and private records protection laws it easily achieved by implementing the right endpoint security system and integrating it in your overall security policy.

A Solution to Emerging Security Risks - CoSoSys Endpoint Protector 2008

Endpoint Protector 2008 is a complete endpoint security solution that can protect your company from all threats that come with portable devices and inside liabilities, while allowing you and your employees to take advantage of all the benefits of modern technology.

The solution is designed to protect your company's PCs from threats posed by removable portable storage and endpoint devices such as USB Flash Drives, MP3 Players, iPods, CD/DVD recorders and digital cameras. These and other devices could be accidentally or intentionally used to leak, steal, or lose data. Endpoint Protector 2008 as a Data Loss Prevention (DLP) is eliminating these risks. Even the introduction of viruses or malware from infected removable storage devices is prevented. Furthermore self-executing devices like a USB Flash Drive with a CD-ROM autorun feature such as U3 Drives will not be controlled and thereby pose no threats.

The white list based approach allows the use of specific devices for certain users or user groups so they stay productive while maintaining control of what devices are used, and what data users are transferring to and from devices.

Endpoint Protector 2008 dramatically reduces the risk posed by internal threats that could lead to your confidential data being leaked, stolen, damaged or otherwise compromised.

Endpoint Protector creates an audit trail that shows the use and activity of portable storage devices in corporate networks. Thus, administrators have the possibility to trace and track file transfers through endpoints and to then use the audit trail as legal evidence for data theft.

Without limiting productivity Endpoint Protector 2008 offers the legitimate use of portable storage devices in a company network while enforcing encryption on all data stored on portable devices when data is being copied to them for transit and use outside the company IT infrastructure.

For more details on Endpoint Protector, please see the Data Sheet available on the company's website http://www.endpointprotector.com.

Conclusions

Business success and significant profits do not depend on a company's size, but in its strategy to make the best of all its advantages, technological or of a different nature. When it comes to security, SMBs cannot afford to cut corners, as the costs of breaches are higher than the cost of proactively addressing possible threats.

As mobility, high end technology and a constant connection to all means of communication power today's business environment, cutting out devices instead of effectively protecting them would be a major strategic disadvantage. That is why endpoint security is the perfect addition to traditional IT security for emerging businesses.

In a world where the use of portable and lifestyle devices is increasingly transforming the way we work and live, Endpoint Protector 2008 is designed to maintain productivity and make work and life more convenient, secure and enjoyable.

About CoSoSys

CoSoSys SRL specializes in network endpoint security solutions, data protection when in transit and portable applications. The solutions portfolio includes functions from encryption, file tracing, biometric security, data synchronization and network security. CoSoSys distributes its products globally through the world's leading hardware manufacturers, software Distributors, Resellers and directly to users at www.cososys.com.

The focus on endpoint threats as part of a complete security policy is a rather new trend. CoSoSys has been focusing on this emerging need ever since 2004, aiming at providing full-circle security solutions against data leaks and other portable device related policy circumvention attempts.

Having a strong business focus on software development, marketing and support of applications working with portable storage devices such as USB Flash Drives and flash based MP3 players, the CoSoSys team has a thorough understanding of their embedded security vulnerabilities. Therefore, CoSoSys has also been developing endpoint security solutions that enable a secure working environment with portable storage devices.

CoSoSys enjoys a continuously growing installation base of users worldwide. The company is headquartered in Cluj-Napoca, Romania and has sales representatives in the United States and Germany.

References

Basel Committee on Banking Supervision, Basel II, http://www.bis.org/publ/bcbs107.htm

Computer Crime Research Center (2005) Security issues: find the enemy within available from: http://www.crime-research.org/analytics/security-insider/

Computerworld.com, Survey: More than 10,000 laptops lost each week at airports, June 2008, http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9105198

Computing.co.uk, Workers Call for IT-enabled Travel, May 2008, http://www.computing.co.uk/computing/news/2217864/workers-call-enabled-travel

Dennis Szerszen, May 2007, Four steps to guard against data leakage from the Endpoint, http://www.securecomputing.net.au/feature/four-steps-to-guard-against-data-leakage-from-the-endpoint.aspx

European Commission, European Union Directive 95/46/EC, http://ec.europa.eu/justice_home/fsj/privacy/

Endpoint Security Info Blog – Archives – April, May, June 2008 http://www.endpoint-security.info/

Federal Trade Commission (2006) ChoicePoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress http://www.ftc.gov/opa/2006/01/choicepoint.htm

Federal Trade Commision, the "Gramm-Leach-Bliley Act" or GLB Act, http://www.ftc.gov/privacy/privacyinitiatives/glbact.html

Gordon L.A., Loeb M.P., Lucyshyn W. and Richardson R. (2005) 2005 CSI/FBI Computer Crime and Security Survey, Computer Security Institute.

Information Commissioner's Office, the Data Protection Act, http://www.ico.gov.uk/

John Leyden / The Registrar, March 2007, Security flap as Scottish council loses USB key, http://www.theregister.co.uk/2007/03/21/perth_council_usb_loss/

John Leyden / The Registrar, April 2006, Afghan market sells US military flash drives. http://www.theregister.co.uk/2006/04/18/afghan_market_security_breach/

Legislative Counsel's Digest, 2002, The California Information Practice Act, http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html

Office for Civil Rights - Health Insurance Portability and Accountability Act (HIPAA), http://www.hhs.gov/ocr/hipaa/

Sandra Kay Miller, March 2007, Gone in a Flash, http://informationsecurity.techtarget.com/magItem/0,291266,sid42_gci1245600,00.html

Sarbanes-Oxley (SOX) Act of 2002, http://www.sec.gov/about/laws/soa2002.pdf

Strategies.gc.ca, The Personal Information Protection and Electronic Document Act, http://privacyforbusiness.ic.gc.ca/epic/site/pfb-cee.nsf/en/h_hc00001e.html

Symantec Corp - Internet Security Threat Report Volume XI (2007, March), http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xi_03_2007.en-us.pdf

Symantec Corp - Internet Security Threat Report (2008, March) http://www.symantec.com/business/theme.jsp?themeid=threatreport

World Intellectual Property Organization, http://www.wipo.int/about-ip/en/

http://www.informationweek.com/security/showArticle.jhtml?articleID=206103872

http://www.theregister.co.uk/2008/01/04/another_stick_with_military_secrets_found/

http://www.theregister.co.uk/2008/02/25/data_breach_real_cost/

http://www.darkreading.com/document.asp?doc_id=146036

Copyright Notice

Contact: **CoSoSys Ltd.**
E-mail: info@cososys.com
Phone: +40-264-593110
Fax: +40-264-593113