White Paper

Secure Passage through a World of Technological Threats

A Guide to Meeting Emerging Security Requirements by Employing **Endpoint Security Solutions**

July 2007

COSOSYS

Table of Contents

Introduction 3

Threats from within.....3

Endpoint Solutions, the Ultimate Goal of Enterprise Security 4

Why Invest in Endpoint Security.....4

CoSoSys: Reliable and Easy to Use Endpoint Security Solutions 5

Endpoint Security and IT Governance 6

Caveats - Managing Employee Discontents 8

CoSoSys: Endpoint Protector Solution.....8

Conclusions.....9

About CoSoSys.....9

References.....10

Copyright Notice.....11

Introduction

Today's business world, in its pursuit for enhanced efficiency, is opening up more and more to all devices that can improve workforce mobility and productivity. Technology has supported our need for mobility and has also provided additional means of communication. Laptops, smart phones, memory sticks, iPods, they are all part of day to day life and work. The downside of this trend is that while largely adopting their usage, few realize how serious the inherent threats are within them, as mobility and portability make data protection a far more complicated problem than ever before.

Portable storage media and personal entertainment devices, such as USB Flash Drives and MP3 players, through their seamless information transfer from and to endpoints (workstations and laptops), generate severe issues when it comes to controlling data use within the enterprise and beyond the physical enterprise boundary. According to the Dieringer Research Group, in the United States alone, more than 44 million were classified as teleworkers, the category including freelancers, contractors, partners or employees traveling or working from home. As a result of such a significant level of (movement) mobility within the workforce, assuring that information stays within the confines of the organization is a major concern.

Threats from within

According to a large number of sources, the most significant security breaches come from insiders,as a result of both malicious and seemingly benign activities. According to the 2005 CSI/FBI computer crime and security survey, the theft of proprietary information went up from $168,529 in 2004 to $355,552 in 2005. Moreover, according to information released by the Computer Crime Research Center in 2005, 98% of all crimes committed against companies in the U.K. had an insider connection While using removable media to steal data from a company or surreptitiously install rogue programs on corporate computers dates back to the days of magnetic tape drives and floppy disks, USB tokens have become a common accessory and also an easy way to either carry data outside a certain enterprise or to make room to serious malware infections, halting activities for hours or days.

Employees play a key role in a company's security and yet many workers do not understand the danger of USB drives. Portable storage devices such as USB flash drives, digital cameras and iPods/MP3 Players are virtually everywhere and are connected to a PC within seconds. Almost every PC has easily accessible USB ports, thus making the theft of data a mere child's play for all network users. Given their need for mobility, employees might see it as their undeniable right to make use of the highly trendy technologies they have access to. For example, an urgent matter requiring significant hours of work from home is interconnected with the employee's ability to move data between home and work computers. The most in handy option would be connecting a plug and play device to the computers USB port and copying all the sensitive data needed for work.

Security Issues Posed by USB drives

Almost 37 % [percent] of businesses surveyed by the Yankee Group in 2005 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.

Also, Symantec's Internet Security Threat Report Volume XI released in March 2007 shows that, in the previous year, theft or loss of a computer or data storage medium, such as a USB memory key, made up 54 % [percent] of all identity theft-related data breaches.
Data theft or infecting the company network through a simple connection is easy and quick. Up to now, network administrators had little chance to prevent this from happening or to identify the responsible user. This was the hard reality until now.

Endpoint Solutions, the Ultimate Goal of Enterprise Security

As a result of demanding security needs that cannot be overcome by traditional security policies and their enforcement mechanisms, endpoint security aims at preventing accidental data leakage and attempts to circumvent corporate data dissemination policies.
The Registrar has recently reported an incident involving a massive confidential data loss caused by a misplaced portable device. According to the IT portal, payment details of Perth and Kinross Council employees where found on a memory stick left in the street. A USB key containing 59 documents, many from the council's Environmental Services Department, were recovered near a bike shelter close to the council building at Pullar House.
As sensitive information can literally walk out the door with the help of barrage from new, portable storage technologies, endpoint security solutions come to strike a balance between strong information security controls and productivity gains from new technologies. Thus, one of the main goals of endpoint security solutions is to ensure the confidentiality, integrity and availability of the information that an organization considers to be sensitive or valuable.

Why Invest in Endpoint Security

For most organizations, implementing additional security solutions can seem nothing more than additional costs. However, preventing possible losses clearly states the advantages of turning to endpoint security as part of the overall enterprise security strategy. For instance, imagine loosing, in a matter of minutes, all the spreadsheets containing confidential information about all your company’s customers. Such a leak would entail severe time loss (phone calls taken in which your employees would have to explain the security breach), loss in customers (many would never again trust your organization and would therefore take their business elsewhere) and possible legal issues. 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, imagine an employee taking some sensitive files home using a Flash Drive. While he or she would only want to catch up with work, the risk of loosing sensitive information is not worth taking. These are only quick examples of the damage that could be triggered by not adopting adequate security measures. Hence, the ultimate goal of endpoint security solutions: endpoint control.

The real threat embedded in portable devices was once again proven in 2006, when flash drives containing classified US military secrets turned up for sale at a marketplace in Afghanistan/Bagram. Shopkeepers claimed the kit was sold to them by cleaners, garbage collectors and other local workers at the nearby US airbase as LA Times, quoted by IT portal The Registrar, reported at the time, flash memory drives from the base were being sold in second hand bins.

The paper further reported that the stolen computer drives could expose military secrets as well as the social security numbers and other personal information of military personnel. This major security breach could have been prevented by using an endpoint security solution. Having sensitive data copied to a password protected / encrypted area of the flash drive would have kept all critical informations safe.

CoSoSys: Reliable and Easy to Use Endpoint Security Solutions

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.

The company products range from home security applications, such as Secure it Easy and Carry it Easy, to complete corporate solutions, offered through the Endpoint Protector suite. Thus, CoSoSys ensures ease of use of modern technology while efficiently protecting the confidential data both at home and within the company.

Endpoint Security and IT Governance

Information Technology Governance, IT Governance or ICT Governance brings a shift of focus in what IT-wise decision-making standards are concerned. While emphasizing the need for desirable behavior in the use of IT within companies, this new concept relates the performance and effective risk management of information technology systems to choosing decision makers carefully and not limiting them to IT departments. The rising interest in IT governance is partly due to compliance initiatives (e.g. Sarbanes-Oxley, Basel II), as well as the acknowledgement that IT projects can easily pose critical security issues and profoundly affect the performance of an organization.

The traditional handling of IT management by board-level executives is, that due to limited technical experience and IT complexity, key decisions are deferred to IT professionals. IT governance implies a system in which all stakeholders, including the board, internal customers and related areas such as finance, have the necessary input into the decision making process. This prevents a single stakeholder, typically IT, being blamed for poor decisions. It also prevents users from later complaining that the system does not behave or perform as expected and/or required.

The primary goals for information technology governance are to (1) assure that the investments in IT generate business value, and (2) mitigate the risks that are associated with IT. This can be done by implementing an organizational structure with well-defined roles for the responsibility of information, business processes, applications, infrastructure, etc. Moreover, adhering to different business standards, be it legal or best practices recommendations, is an important part of IT Governance.

CoSoSys' Endpoint Security Solutions can help your enterprise meet the requirements of the following legislation acts, international standards and compliance initiatives:

HIPAA (US)

In 1996, Congress enacted the Health Insurance Portability and Accountability Act (HIPAA). A key goal of HIPAA is to protect medical records by establishing transaction standards for the exchange of health information, security standards, and privacy standards for the use and disclosure of individually identifiable health information.

SOX (US)

The Sarbanes-Oxley (SOX) Act of 2002 was developed to protect investors by improving the accuracy and reliability of corporate disclosure. Section 404 of the Act requires all public companies to assess and report on the effectiveness of internal controls and procedures for financial reporting, including access and dissemination of sensitive financial information.

GLBA (US)

The Gramm-Leach-Bliley Act, also knows as GLBA, seeks to protect the personal information of consumers stored in financial institutions. The Act requires all financial institutions to implement and maintain security measures to protect customer information and prevent unauthorized access and use of customer records.

PIPED (Canada)
The Personal Information Protection and Electronic Document Act mandates that appropriate security measures be applied to personal data obtained on the course of commercial transactions.

SB 1386 (California, US)
The California Information Practice Act or Senate Bill 1386 that went into affect on July 2003 requires state agencies or companies that conduct business in California and own or license computerized personal information, to disclose any breach of security to any resident whose unencrypted data is believed to have been disclosed.

95/46/EC (Europe)
European Union Directive 95/46/EC is a sweeping European Parliament directive designed to protect individuals from unregulated personal data access or transfer.

DPA (UK)
The Data Protection Act mandates that the processing of sensitive personal data should be carried out with appropriate security in the interests of protecting the individual rights and privacy. DPA prohibits the disclosure of personal data to any third party without the explicit consent of the targeted subject.

Basel II(Europe)
Basel II is the second of the Basel Accords, which are recommendations on banking laws and regulations issued by the Basel Committee on Banking Supervision. The final version aims at ensuring that capital allocation is more risk sensitive, separating operational risk from credit risk, and quantifying both, attempting to align economic and regulatory capital more closely to reduce the scope for regulatory arbitrage.
Basel II establishes minimum capital requirements for banking organizations to reduce operational risks, defined as the risk of loss resulting from inadequate or failed internal process, people and systems or from external events. To achieve compliance with Basel II requirements, organizations must identify, assess, monitor and control their operational risk, much of which occurs at the endpoint.

Caveats - Managing Employee Discontents

As stated earlier, employees may see it as their undeniable right to carry sensitive information from and to the office. Therefore, some may reject the newly implemented endpoint security solution, as they might see it as imposing unwanted and unnecessary limitations. The best way to handle such issues is to make the benefits of using Endpoint Protector known to your staff.

While lack of information can lead to a large number of misunderstandings, employees are rarely unreasonable. Being able to provide all needed details, best practices, and emphasizing the benefits of the enhanced enterprise data safety enabled by your endpoint solution will be enough to handle any emerging issues. Company policies, be it security or behavior related, must be comprehensive and integrated in building your image and company culture.

CoSoSys: Endpoint Protector Solution

Endpoint Protector gives network administrators back the control needed to keep network endpoints safe.

- Control use of all USB storage devices
- Tracking of what data is saved to USB storage devices
- Tracking of what data is copied from USB storage devices
- Authorize the use of USB storage devices Trusted Devices™
- Securing data on USB storage devices
- Powerful reporting tool

CoSoSys' Endpoint Protector is the only solution that gives corporations the ability to let the network users use the increasingly important functionality of the USB Port without loosing control over data.

The CoSoSys endpoint solution is designed to control usage of all USB storage and to also keep track of what data users are taking from and to their work computers to any kind of portable USB storage devices. Furthermore, Endpoint Protector enables network administrators to monitor and report what data is introduced into the corporate network from a portable storage device such as prohibited material (such as MP3s, movies or games) or harmful data like a virus that could jeopardize the networks integrity.

As not all portable storage devices are used with the intent to harm the company, many legitimate reasons common justify the need of such devices to increase networks users' productivity. Endpoint Protector thus allows authorized use of "Trusted Devices" such as the companies' own USB Flash Drives to copy and transfer data.

To ensure the protection of data carried by users on "Trusted Devices", Endpoint Protector allows users to copy work data to a password protected / encrypted area of a "Trusted Device" only, so that confidential corporate data is protected in case of a hardware loss.

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.

For more details on Endpoint Protector, please see the Data Sheet available on the company's website.

Conclusions

As information theft and proprietary data leakage are a reality of today's business world, effectively preventing all possible security breaches is becoming an ultimate concern for enterprise security experts. Endpoint security comes to complete your existing security policies, aiming to render it full proof.

As new circumvention and data compromising techniques come to diminish the benefits of new devices and gadgets, Endpoint Protector secures your company's technologically enabled mobility. Thus, by easily protecting all exposed endpoints from inbound and outbound threats, you can enjoy enhanced portability, efficiency and productivity.

As it enables your employees to use devices you have already invested in and it protects your company from losses generated by attacks from outside and within, all financial costs entailed by implementing Endpoint Protector, such as purchase, implementation and usage training expenses, are fully justified by the yielded return on investment.

About CoSoSys

CoSoSys SRL is specialized in the development of software for portable storage device enhancement and network endpoint security. The application portfolio includes functions from password security, data synchronization and network security. CoSoSys distributes its products globally through world's leading hardware manufacturers, software Distributors, Resellers and directly to users at www.cososys.com. 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/ (last cited 28 July 2006).

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/

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 (last cited 27 July 2006) 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

Copyright Notice

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