SPECIAL ADVERTISING SUPPLEMENT

White Paper

content technologies

MIMEsweeper

Executive Insights on Content Security:

Proactively Addressing Potential Liabilities in the New Economy

IDC
INTERNATIONAL DATA CORPORATION

COMPUTERWORLD
CUSTOM PUBLISHING

Executive Insights on Content Security:

Proactively Addressing Potential Liabilities in the New Economy

By Richard Dean, Program Manger, and Allan Carey, SeniorAnalyst, IDC

During the first half of this year, a number of high profile incidents were featured in the media which detailed malicious intruders sabotaging Web sites. Widely recognized names such as eBay, Amazon.com and E*Trade experienced significant downtime costing millions of dollars in lost revenue. Because of these incidents, security has become a major concern for every top-level executive whose business is increasingly dependent on e-commerce.

However, information security is not limited to e-commerce. It is also relevant to all Internet activities including e-mail and Web browsing. As more businesses provide Internet access to employees, content security and the potential liabilities surrounding unrestricted access are being discussed in executive boardrooms.

Issues Business Executives Face

Emerging technologies and the Internet are designed to allow businesses to be more productive and efficient. E-mail is the most widely used means of business communication, both internally and externally, because it is very intelligible and only requires a computer with a simple mail program and an Internet connection. The Internet has proven to be an evolutionary tool to gather competitive market information, prospect for sales leads, attract new customers, build stronger relationships with existing customers and suppliers and develop new distribution channels. These technologies also expose companies to an entirely new realm of liabilities and vulnerabilities.

In a recent study conducted by the American Management Association (AMA), 64% of employees, on average, have access to e-mail. E-mail penetration has saturated the enterprise market while opportunity for growth still exists in the small to medium sized business markets. With e-mail access literally at their fingertips, employees can correspond with friends and family aside from conducting their regular business activities. Of course, employees can also receive e-mail from any source through the Internet.

When an unsuspecting employee opens new e-mail, it can be like opening Pandora's box. For some hackers, e-mail is their transport vehicle of choice to hide worms, viruses and malicious mobile code (MMC). There have been numerous highly publicized cases including the "I Love You" bug, its mutant strain "Love Letter", and the infamous "Melissa" virus. By using a Trojan horse technique, hackers can gain access to the vital corporate infrastructure allowing vicious programs to wipe out hard drives, attach themselves to stored e-mail addresses and forward themselves to other unsuspecting recipients, and cause mission-critical data to be lost. The ramifications can be devastating. Estimates suggest that viruses alone have caused worldwide damage reaching $11 billion due to lost employee productivity, downtime and data loss.

According to the AMA report, 48% of employees have access to the Internet. Apart from conducting business activities on the Internet, employees have the freedom to browse their favorite Web sites, shop online and conduct personal financial transactions. These are the types of activities that can cause valuable and costly bandwidth to be consumed.

Other temptations of the Internet include pornographic sites, racially discriminatory sites and other pitfalls that can expose businesses to a multitude of legal liabilities. Underscored by the recent dismissal of dozens of Dow Chemical employees, companies are taking a no-tolerance posture involving the sending or storing of pornographic or violent e-mail materials within the workplace. Since July, Dow Chemical is reported to have terminated or disciplined nearly 300 employees for violating company policy regarding obscene e-mails. Prompted by an employee complaint, Dow narrowed its investigation by filtering keywords to locate potentially offensive materials, which were then further reviewed for violations.

Together, e-mail and the Internet can equal lost productivity, which in turn can quickly bring about a reduction in profitability (See chart). The $9,600 figure from the chart may not seem significant, but when multiplied by 1,000 employees, the result is $9.6 million lost in productivity. The total excludes all costs associated with providing Internet access.

Potential Losses Resulting from Declines in Employee Productivity

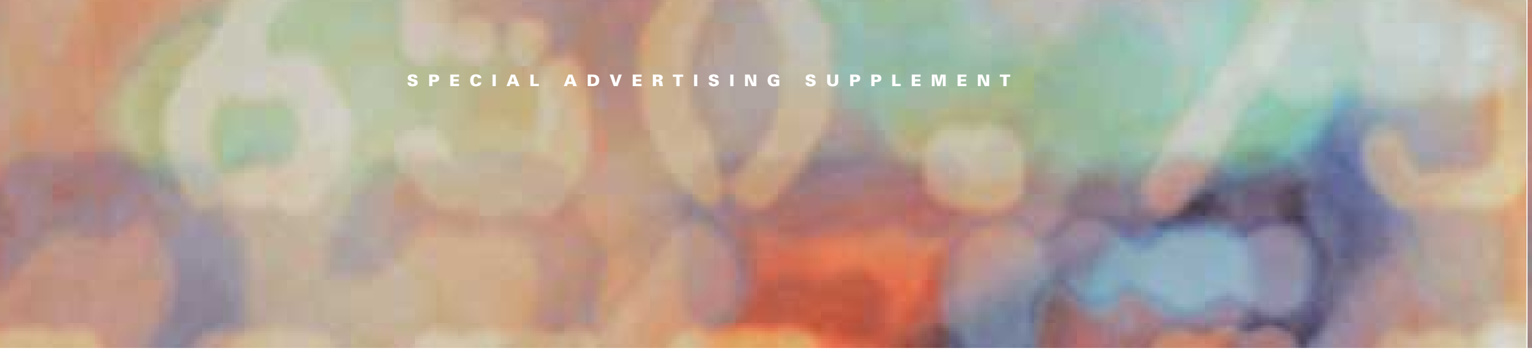
FACTORS	RESULT
Number of hours per day each employee spends on personal business	**1**
Number of work days per year	**240**
Average hourly rate including overhead expenses	**$40**
Annual cost of lost productivity per employee	**$9,600**

SOURCE: INTERNATIONAL DATA CORP., FRAMINGHAM, MASS. 2000

Another issue employers must face is employer's rights vs. the employee's right to privacy. It has become a very fine line for the employer to walk. Due to global resource constraints, employees are spending an increasing number of hours at work, often leaving little time to accomplish duties required in their personal lives. Consequently, employees end up using company time and equipment, primarily e-mail, the Internet and a PC, to fulfill these personal duties. Does management consider this to be an acceptable or a fair trade-off between employees working more hours and employees using company assets for personal use? For many companies today, the privacy issue produces a pendulum effect swinging between an acceptable level of personal activity in the workplace to one side and a flagrant abuse of company assets to the other side.

This workplace dilemma also leads to the question of whether or not employers have the right to monitor employees' activities utilizing content security initiatives when these employees are using company assets. Do employees have the right to expect a certain level of privacy while on the job? There are valid arguments from both sides of this quandary. Employers believe they not only have the legal right, but the obligation, to monitor all activities within the confines of the physical surroundings as well as with company-owned assets. Today, the clash of both standpoints is being fiercely debated in many executive boardrooms, with employee rights groups and within certain legal circles.

In addition to privacy rights, businesses are confronted with the illicit siphoning of trade secrets. Proprietary infor-



mation remains a significant security concern for many CEOs. In 1998, for example, the Department of Commerce (DOC) reported that U.S. businesses incurred $12.5 billion in intellectual property losses.

Statistics indicate company insiders are often responsible for the majority of damage. These insiders can be current or former employees with motives such as revenge, self-promotion, notoriety or financial gain. If employees continue to have unlimited access to information without a comprehensive content security initiative in place, millions of dollars worth of intellectual capital could be trickling out of the business undetected.

It is critical, therefore, for business decision-makers to consider the drawbacks of monitoring employees' activities when evaluating whether or not to develop a content security initiative. The process is often time-consuming and labor-intensive. Dedicated human resources are needed to review all e-mails flagged for suspicious activity and to subsequently determine appropriate actions. Internet usage records require a similar review and evaluation process. This can be a costly endeavor to ensure a secure and productive ebusiness environment. The question becomes, which is the lesser of two evils? Investing to keep the environment secure? Or investing to replace what is lost or stolen from the environment?

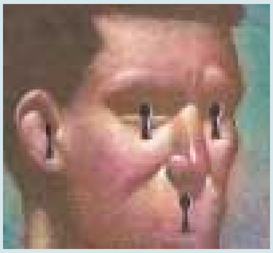
Content Security

In order to ensure a secure and productive ebusiness environment, while protecting employee privacy, business decision-makers can implement a comprehensive content security policy imbedded in the early stages of business policy formulation. Content security picks up where anti-virus leaves off. It involves an Internet management tool utilized to control and manage e-mail scanning and monitoring, Web content and downloadable applications execution. The tool also offers customization functionality based on corporate policies. The content can be both active and passive. Examples of active content include viruses, Trojan horses, ActiveX, executables (.exe) and malicious mobile code. Passive content includes e-mail and excessive use of bandwidth. In addition to archiving, encryption and image scanning, the functions of content security are:

- E-mail scanning and monitoring – Checks all e-mail — inbound and outbound — for confidential data, excessive file size and proprietary material. Messages are scanned using keywords and phrases.
- Web content – Checks all Web activity by identifying and managing Web content containing racist or hate material, banned files, pornography, profanity and potentially lost or corrupted material.
- Downloadable applications execution – Checks all content for viruses, Java scripts, ActiveX and .exe. These can be attached to e-mails or hidden behind downloadable material from the Web.

A comprehensive content security initiative involves participation from the employer and the employees to ensure adoption and success of the program. The main components of a comprehensive program include the following elements:

- Establish a content security policy – A company policy that defines electronic usage for employees and warns them about acceptable business practices when using company assets and the repercussions for violating the policy. This policy covers all e-mail correspondence, Internet usage and appropriately sets employees' expectations of privacy. Employees are warned that monitoring takes place and each employee signs a consent form. A successful policy requires involving employees early in the process, gaining their buy-in and being flexible with expectations.
- Education and training – By educating employees and raising awareness of security issues, employees better understand the benefits of a content security program.
- Content security solutions – These solutions enable businesses to identify and manage content access over the Internet.



Ripped Off

Theft of intellectual property most frequently occurs through the following groups:

- Insiders
- Intruders
- Hacktivists
- Criminals
- Industrial espionage
- Government-sponsored activity

SOURCE: DEPARTMENT OF COMMERCE

Allan Carey is senior analyst and Richard Dean is program manager for Framingham, Mass.-based International Data Corp.'s Information Security Services research program. For more information on Content Security, see IDC's white paper, Content Security: Policy-Based Information Protection and Data Integrity.

Many vendors offer these solutions, including Content Technologies, Tumbleweed and Trend Micro.

- Maintenance and review – As businesses change, company policies are updated to ensure business and network integrity in the ebusiness environment. Content security solutions are modified to address new threats and hazards.

Implementation of a comprehensive content security program will help ensure a secure ebusiness in an "always on" global economy. By taking the three e's — establish, educate and enforce — approach to content security, businesses gain a high degree of confidence, while fostering a harmonious and trusting work environment.

Risks of Disregarding Content Security

A plethora of issues can arise if a security program is not implemented. It can expose the company to an overwhelming number of legal and financial problems. Below are a few issues executives need to consider:

- Class and individual action suits
- Loss of network integrity and availability
- Loss of intellectual capital
- Loss of employee productivity
- Defamation of brand name and reputation

Class and individual legal action in the form of sexual harassment and hostile work environment, invasion of privacy and wrongful termination are examples of the most common legal liabilities. An illustrative case was Bouke vs. Nissan Motor Co. (1991). Two employees were terminated for having e-mail containing inappropriate language and jokes. The employees sued for invasion of privacy because the e-mails were obtained through monitoring. The judge ruled in favor of the defendant because Nissan required employees to sign a consent form explaining the company usage policy. The employees were aware that the company hardware and software were only intended for business use and that the company was monitoring information transfers.

Another example was New York State Correction Officers and Police Benevolent Association vs. State of New York Department of Corrections (2000). In this case, union members are suing the State of New York for exposing confidential information about the correction officers to inmates. The confidential information consisted of social security numbers, addresses and other personal information. The union is suing for an unspecified amount in damages. This is a provocative example of potential liability due to unsecured data.

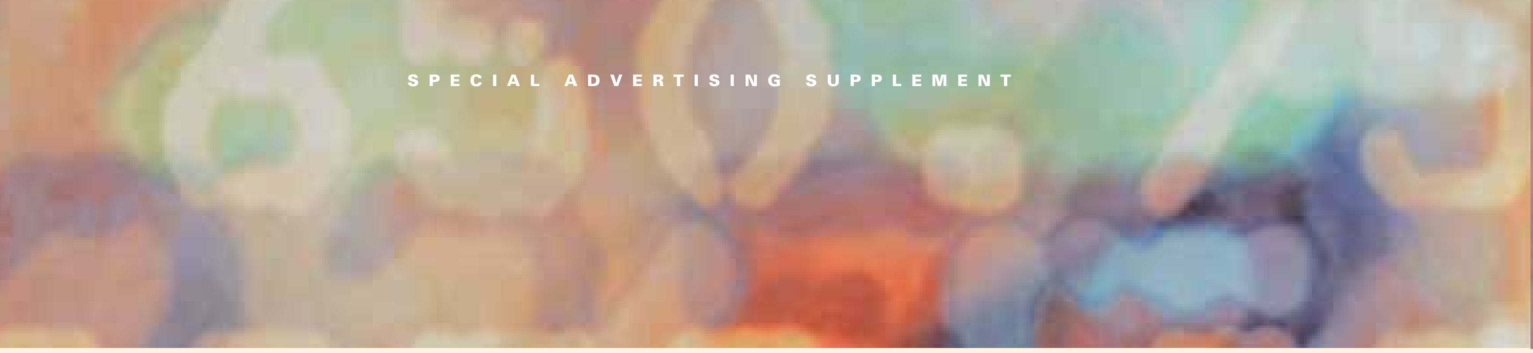
When viruses, executables or malicious mobile code compromise network integrity and availability, mission-critical data can be lost or stolen without detection. One malicious attack can wreak havoc causing millions of dollars in lost revenue, not to mention the potential loss of intellectual capital. Reports estimate 97% of all ebusiness crimes go undetected or unreported. If a criminal breaks into a home, a homeowner would report the intrusion to the proper law enforcement authorities. Why wouldn't the same thought process apply to the business?

Businesses often refrain from divulging their vulnerabilities in order to prevent unwanted notoriety and additional attacks and businesses can't afford to blemish their reputation and brand name. It takes seven times more effort and money to attract new customers than it does to hold on to existing ones. In the ebusiness world, trust and loyalty are critical attributes to protect.

Breaches of security can become the catalyst for severe economic upheaval. Therefore, content security should be integral to the strategic business plan to safeguard against the potential legal and financial liabilities inherent with business activities conducted over e-mail and the Internet.

Adding to the argument, the return on investment (ROI) attributed to proactively implementing a content security plan is quantifiable from both an economic and human resource perspective. Essentially, businesses reap the monetary benefits of establishing a comprehensive program through increased employee productivity, improved network integrity and availability, stronger relations with partners and suppliers, and increased profit potential. In addition, businesses cultivate knowledgeable employees who are aware of and can guard against the trappings of the Internet.

Finally, senior executives also earn the respect, trust and loyalty of the workforce by establishing an environment of open communications. In such an environment, both employee and employer understand expectations and can work toward reducing potential liabilities and promoting the goals and objectives of the organization.



CASE STUDY: ZENITH ELECTRONICS CORP.

Content Technologies' MIMEsweeper Keeps E-mail Clean at Zenith

The hottest growth area in the field of Internet security is content security, with expected compound annual growth of 71% from 1999 to 2004, according to Framingham, Mass.-based research firm International Data Corporation (IDC). Content security revenues were only $66 million in 1999. In 2004, IDC expects that number to reach almost a billion.

The Critical Need

The reason for this fast growth: content security addresses a critical need in virtually every company connected to the Internet — a need that only recently was widely recognized. Viruses, pornography, oversized files or banned file types, spam and malicious Java code are innocently downloaded from a Web site — there are lots of dangers lurking out there in cyberspace — dangers that can bring down networks, spur harassment lawsuits, and degrade productivity of both people and systems.

Just think of the people who got hit hard with the Melissa virus, or any of the new ones that came out. We don't have to worry because MIMEsweeper catches new viruses even if we haven't updated the virus definitions.

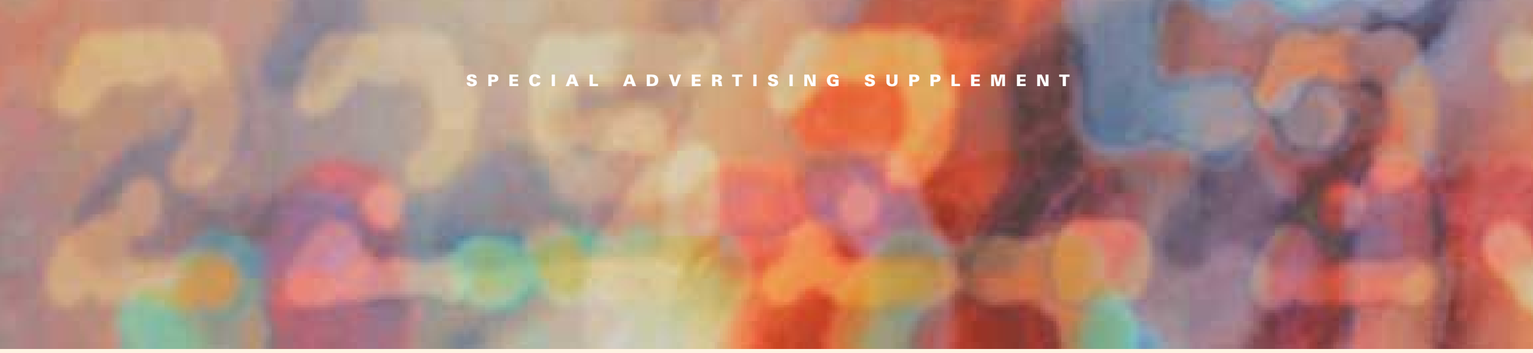
-Jeff Ferrera, e-mail administrator, Zenith Electronics Corp.

Employees can unknowingly or deliberately send trade secrets to a competitor with the click of a mouse. Content security products protect companies from these dangers by scanning content and stopping suspect e-mail or Web downloads before they do damage.

Of course, some companies have been wise for years to the content dangers posed by the Internet. Zenith Electronics Corporation is a case in point. A developer and user of technology since its founding in 1918, the Glenview, Ill.-based company had 1999 sales of $834 million. Over four years ago, Zenith was one of the first companies to install Content Technologies' MIMEsweeper when it was first introduced.

MIMEsweeper scans all e-mails coming into or out of the organization through a dedicated Microsoft Windows NT box. Once through the gateway, e-mail is sent to the local network in Glenview or over leased lines to other locations. Any e-mail that violates policies set by Zenith is automatically blocked. Depending on the violation, the e-mail may be discarded, bounced back to the sender or held for further analysis by the IT staff.

"I can't remember the last time we had a virus in here. MIMEsweeper looks for things like Java script HTML viruses, Visual Basic stuff, .exe files — all the things that can attach to an e-mail. Usually, it can clean the e-mail for me — it will actually go in and blow up the attachment long enough to clean the virus, wrap the attachment back into the message, and send it on its way," says Jeff Ferrera, Zenith's e-mail administrator.



The Greatest Benefit

MIMEsweeper's greatest benefit is peace of mind.

"Just think of all the people who got hit hard with the Melissa virus," says Ferrera. "Or any of the new ones that have come out. We didn't have to worry because MIMEsweeper catches new viruses even if we haven't updated the virus definitions, which I probably don't do as often as I should. Every now and then I'll walk in the office in the morning and someone will say 'Oh, did you hear about such and such new virus that's going around?' and I'm thinking in my head that there is probably a new virus definition I should have downloaded. Then I will go to the [Windows NT] box and find that MIMEsweeper is already catching the infected messages," he says.

Virus Updates

Not that updating the virus definitions is all that difficult, Ferrera says. Rather than reinvent the wheel, MIMEsweeper works with the anti-virus detection product an IT organization may have already installed, invoking that product to detect and cleanse a specific virus when it thinks one is present. Zenith, for example, uses the Command Software (Jupiter, Florida) Virus Scanner for MIMEsweeper. "To update the virus definitions all I need to do is download them from the Command Software Web site," Ferrera says.

But Zenith doesn't take any chances when it comes to attachments. "If an e-mail comes in here with an attachment containing, say, a Visual Basic script that it doesn't recognize, MIMEsweeper has instructions to hold the message until I've looked at it," Ferrera says. "Typically what I'll do is check out the message to see if it looks okay before releasing it to the intended receiver."

Greater Control over E-mail

Ferrera also likes MIMEsweeper because of the control it gives Zenith over its e-mail traffic in general. For example, it can detect who's sending or receiving the most mail — which allows better resource deployment and load balancing. MIMEsweeper also helps Zenith to accurately and quickly diagnose user e-mail problems.

"We also use MIMEsweeper for scanning outgoing mail," states Ferrera. "I can think of one case in particular where we had an employee leave us who began soliciting his ex-Zenith colleagues to join him at his new place of employment. So we blocked all incoming mail from that sender.

Given the need, the system can also be used to scan all e-mail content for a particular phrase to protect against loss of trade secrets, or to block people from sending or receiving e-mail to or from specific addresses."

More Than a Sense of Security

MIMEsweeper can also help users with issues other than security related topics.

"Actually, someone came to me today — they were sure their e-mail had been lost. I was able to check the log files and see that, yes, the e-mail had come in but it had been mis-addressed," he says.

MIMEsweeper had not only held the mail, it had sent a message to the sender notifying them of the error.

"I would consider MIMEsweeper to be a 'must-have' for any organization," Ferrera says, "if only to protect yourself. I think the product is invaluable."

COMPUTERWORLD
CUSTOM PUBLISHING

This White Paper on Content Security was created by Computerworld's Custom Publishing group. Comments on this supplement can be sent to managing editor Stefanie McCann at (508) 820-8234 or stefanie_mccann@computerworld.com. This White Paper, as well as other custom supplements, can be viewed online at www.computerworld.com.