White Paper

SurfControl®

The Global Push to Protect Confidential Information Online

a SurfControl White Paper

with contribution by Hammonds

The World's #1 Web & E-mail Filtering Company

Table of Contents

Material presented in this white paper is a summary of selected existing laws as of October 2003. It should not be relied upon as legal advice.

The Global Push to Protect Confidential Information Online

Introduction

An estimated 62 percent of employed Americans have Internet access at work and virtually all of those use e-mail on the job. That's more than 57 million adults in the United States with e-mail access at the office.[1] Users now view e-mail as more important than the phone for carrying out daily business tasks, a recent survey found.[2] As indispensable as e-mail and the Internet have become at work, companies face rising threats from the exposure of confidential business or consumer data over the Internet.

Rarely does a month go by without headlines detailing electronic breaches of confidentiality. In February 2003, a hacker violated the security of a credit card processor's database containing eight million American Express, Discover, MasterCard, and Visa account numbers.[3] In April 2003, Eli Lilly and Company settled U.S. charges that it disclosed 669 e-mail addresses of Prozac users.[4] In 2002,Cisco inadvertently released a memo on quarterly earnings before the information was made public[5] and Hewlett Packard fired an employee who leaked internal memos about the company's status while the company was in merger talks.[6]

The disclosure of confidential information - whether accidental or intentional -- nearly always tarnishes the reputation and the business of the company involved.

The disclosure of confidential information – whether accidental or intentional -- nearly always tarnishes the reputation and the business of the company involved.

- Theft of proprietary business information is on the rise and companies are often caught by surprise when they learn the identity of some of the culprits – their own disgruntled employees.
- When confidential business information is leaked prematurely, market capitalization and stock prices can plummet, competitors can benefit and revenues can suffer.
- Companies can face legal liability from the online activities of employees, from harassment lawsuits to six-figure settlements stemming from the traffic in illegally obtained copyrighted music or movies.
- Consumers say they will react to the exposure of private personal information – even inadvertent – by pulling their brand loyalty, giving their business to competitors and avoiding doing business online.

---

[1] Pew Internet & American Life Project, December 2002, "Email at Work" by Deborah Fallows (www.pewinternet.org/reports/pdfs/PIP_Work_Email_Report.pdf)
[2] The Meta Group, June 5, 2003, "E-Mail Concerns in 2007" by Matt Cain
[3] The Associated Press, February 19, 2003, "Hacker tapped Omaha firm's computers to get credit card numbers" by Barry Bedlan
[4] The Computer & Internet Lawyer, April, 2002, "Eli Lilly Settles FTC Charges Concerning Disclosure of Email Addresses of Prozac Users"
[5] Securities Litigation & Regulation Reporter, January 2, 2003, "The Fear Factor of Corporate Responsibility" by Betsy Atkins
[6] Ibid

Corporate content security is more than just a form of public relations. It's now the law.

In nearly every country in the industrialized West, protection of business and consumer information is governed by new laws and regulations. These laws protect consumers, requiring companies to safeguard financial information, health-care records, and personally identifying data. Other regulations dictate what sensitive business information can be disclosed, to whom and when. Multi-national corporations, in particular, need to be aware that the nature of protected information may vary from country to country. That is significant because e-mail and the Internet have made the nature of many businesses global and there are now a growing assortment of national laws on the books that require businesses to exercise caution or suffer civil fines, criminal penalties, and other serious business consequences.

Best practices for content security involve a three-pronged approach: combining risk assessment, internal policy development, and technology initiatives.

Given the new legal paradigm, companies are realizing that they cannot leave their electronic content unsecured – no more than they would leave computer networks unprotected from viruses, spam, or hackers. Best practices for content security involve a three-pronged approach: combining risk assessment, internal policy development, and technology initiatives. Companies need to determine what electronic content is being generated. They must develop company policies regarding who has access to data, why, and what state or federal regulations they must meet. The cornerstone of this strategy is to employ a technological component that enforces the rules and ensures regulatory compliance. The sheer volume of e-mail, instant messages, and peer-to-peer communications rules out traditional safeguards, such as manual key word entry. According to IDC, the market for content security software – most notably messaging security products such as e-mail and instant messaging filters and content recognition tools – has exploded, jumping 49 percent in one year to $506 million in revenues worldwide in 2002.[7] A review of global laws and regulations makes it easy to understand why.

The U.S. approach to confidentiality protections online: from self-regulation to legislation

Internet commerce was barely out of its infancy in the United States when firms began to collect and process personal data online. Data such as names, e-mail addresses, and purchase history was useful not only in assessing how a company might improve goods or services, but as a commercial asset for marketing or licensing to other parties. At the same time, the ability to quickly transmit that information around the globe or marry it with other data posed unprecedented threats to consumer privacy. Companies could build customer profiles in order to target advertising or pricing. But the information also became vulnerable to identify theft and fraud and worries increased as more sensitive information – such as financial and medical records – moved online.

In Washington, D.C., in the mid-1990s, the Clinton Administration worked to stave off blanket Internet privacy regulations in favor of persuading e-commerce firms to adopt voluntary privacy policies and practices to alleviate consumer fears about transactions in cyberspace. The U.S. Federal Trade Commission enforces those policies and has brought cases against companies, ranging from clothing manufacturer Guess Inc. to software giant Microsoft, over the

[7] IDC, July 2003, "Content Security: The Business Value of Blocking Unwanted Content" by Brian E. Burke

misrepresentation of privacy policies regarding consumer data on their Web sites.[8] But the continuing headlines detailing corporate disclosure of private information convinced Congress that it needed laws to protect some forms of information collected online – financial data, medical information, sensitive business information, and, most recently, links to suspected terrorist organizations.

The laws that now exist to protect confidential information in the U.S. were developed in different segments.

- **Consumer financial data**

Concern about the collection and use of sensitive financial data – such as bank and credit card account numbers, income and credit histories, and social security numbers that can be linked to names and addresses – led to the Financial Modernization Act of 1999, also known as the Gramm-Leach-Bliley (GLB) Act. GLB requires financial institutions to safeguard the confidentiality of this information. The act was broad enough to include mortgage brokers, real estate appraisers, professional tax preparers, ATM operations, and a host of other businesses in addition to banks and investment houses.[9] Penalties for non-compliance can range up to $11,000 per day and $10,000 per violation.

Selected U.S. Laws	
Gramm-Leach-Bliley, Fair Credit Reporting Act	consumer financial data
HIPAA	medical and health care information
SEC Regulation FD & Rule 17a-4; Sarbanes Oxley	business information, corporate governance
USA Patriot Act	suspected terrorist links

Congress is still working on modifications to another law, the Fair Credit Reporting Act (FCRA), to give consumers tougher federal protections against identity theft, increased access to their credit reports, and the ability to "opt out" of receiving marketing and other solicitations.

Both FCRA and GLB outline an exhaustive number of steps that companies must take to ensure that they protect this information, including: designating and training one or more employees to coordinate the safeguards, assessing the risks to customer information collected by the company, and designing and implementing a safeguards program. Notifying employees of the rules and training them to safeguard the data is imperative, but time and again it has been human failure more than technology that has resulted in accidental or intentional disclosures of confidential information.

- **Medical and health-care records**

To U.S. lawmakers, another area of concern became the security of medical records as hospitals, insurance carriers, and doctors' offices shifted from paper to electronic records during the mid-1990s. In this case, too, the push for legislation was in part prompted by embarrassing disclosures of patient information, from identifying information about AIDS patients or drug users to one case where a university released the names of deceased organ donors to 410 kidney recipients.[10]

[8] http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html
[9] Financial Privacy: The Gramm-Leach-Bliley Act (http://www.ftc.gov/privacy/glbact/)
[10] The Associated Press, January 15, 2002, "Minnesota patients inadvertently receive names of organ donors"

The Congressional Health Insurance Portability and Accountability Act (HIPAA) of 1996 contains provisions to give patients more control over the accuracy of medical information and sets boundaries on health plans, health-care providers, and clearinghouses involved in the payments process.[11] But it also sets out safeguards that health-care providers must meet to keep this information confidential. These provisions, which went into effect in April 2003, hold violators accountable with civil penalties of up to $25,000 per year and/or criminal penalties for illegally obtaining protected health information, of up to $250,000 in fines and 10 years in prison, if the intent is to sell or use the data for commercial advantage or to cause harm.[12]

- **Sensitive business information**

Recent allegations of malfeasance against officers at Enron, WorldCom, Global Crossing, Imclone Systems, and at the Wall Street investment banks that drummed up investor interest in such companies convinced lawmakers and regulators to seek greater transparency for the public in the financial operations of publicly listed companies. A series of laws and regulations now exist governing what records publicly traded companies must keep, when they must file this information with regulators or make it available to the investing public. Other rules spell out what information and communications are required to be kept by brokers and dealers who trade in these companies. These rules were developed in reaction to a series of public scandals starting in 2001 involving allegations of insider trading, accounting fraud, and lack of oversight of executives by corporate boards.

The new rules require companies to better police the creation, retention, and dissemination of electronic records. The U.S. Securities and Exchange Commission was one of the first on the bandwagon with Regulation FD, which bars the selective disclosure of material nonpublic information, regulates trades by insiders, and further defines when traders or brokers or family or non-business relationships give rise to liability under insider trading rules.[13] The SEC also sought high-profile prosecutions under Rule 17a-4 requiring the retention of records and communications by broker dealers for up to six years following scandals at investment banks that had destroyed some of these records before coming under federal and state probes. In December 2002, the SEC, NYSE, and NASD imposed $8.25 million in fines on five firms – Deutsche Bank Securities, Goldman Sachs, Morgan Stanley, Salomon Smith Barney, and U.S. Bancorp Piper Jaffray.[14]

Congress also reacted to the corporate scandals. The Sarbanes-Oxley Act of 2002 defines standards for tracking and reporting that are intended to better hold accountable CEOs, CFOs, and directors of publicly traded companies for their financial statements. Potential penalties range from personal fines to prison terms of up to 10 years, or both.[15] Section 404 of Sarbanes-Oxley requires CFOs to attest to their companies' internal financial controls and "provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition,

---

[11] HIPAA Guidance from CDC and Health and Human Services (http://www.cdc.gov/mmwr/preview/mmwrhtml/m2e411a1.htm)
[12] Department of Health and Human Services, "Protecting the Privacy of Patients' Health Information," (http://www.hhs.gov/news/facts/privacy.html)
[13] U.S. SEC, "Final Rule: Selective Disclosure and Insider Trading" (http://www.sec.gov/rules/final/33-7881.htm)
[14] U.S. SEC, December 3, 2002, "SEC, NYSE, NASD Fine Five Firms Total of $8.25 Million for Failure To Preserve E-Mail Communications" (http://www.sec.gov/news/press/2002-173.htm)
[15] U.S. SEC, Spotlight on Sarbanes-Oxley Rulemaking and Reports (http://www.sec.gov/spotlight/sarbanes-oxley.htm)

use, or disposition of the registrant's assets."[16] One of the major threats to data in those systems can be e-mail and attachments. About 85 percent of all public companies intend to alter or upgrade their information technology systems as a component of complying with Sarbanes-Oxley alone, according to an April 2002 survey conducted by AMR Research Inc. Those companies could spend $2.5 billion in 2003 on IT projects linked to compliance.[17]

- **Suspected terrorist links**

In response to the terrorist attacks on Sept. 11, 2001, Congress approved the USA Patriot Act, which gives federal officials greater authority to track and intercept communications for law enforcement and foreign intelligence gathering. One provision vests the U.S. Department of Treasury with regulatory powers to fight people or groups that may use U.S. financial institutions for money laundering. Banks, credit unions, and other financial institutions now must gather personal data – name, address, tax ID, date of birth, and a copy of a government-issued photo ID – in order to verify the identity of account holders and determine that these people or institutions are not on any terrorist watch lists. While the government was given greater access to this data under the new law, these financial institutions are now burdened with maintaining the information for at least five years and protecting against its dissemination or misuse.[18]

The European Union: Laws standardizing consumer privacy protection

In the European Union, protection of consumer privacy took center stage as lawmakers sought to standardize personal data management laws throughout the 15 member states. After the European Parliament approved the Data Protection Directive in 1995, a series of national laws were developed – and are, in some cases, still evolving. They require companies that collect data to register with national data protection authorities, to legally obtain customer data, and use data only for specific purposes, among other requirements.[19] In some countries, tougher protections were put in place, barring collection of certain types of sensitive data – about religion, sexual attitudes, or health – without pre-approval.

The E.U. directive and the country-specific laws pose potential problems for multi-national companies. Companies are required to register with the national data protection authorities and comply with the directives in each country in which they do business.

The E.U. directive and the country-specific laws pose potential problems for multi-national companies. Companies are required to register with the national data protection authorities

[16] U.S. SEC, "SEC Implements Internal Control Provisions of Sarbanes-Oxley Act" (http://www.sec.gov/news/press/2003-66.htm)
[17] CIO Insight, August 8, 2003, "Sarbanes-Oxley: Comply With Me" by Gary Bolles
[18] U.S. Department of the Treasury, Sept. 13, 2003, "Final Regulations Implementing Customer Identity Verification Requirements under Section 326 of the USA PATRIOT Act" (http://www.treasury.gov/press/releases/reports/js7432.doc)
[19] European Commission, Data Protection (http://europa.eu.int/comm/internal_market/privacy/index_en.htm)

and comply with the directives in each country in which they do business. In addition, the E.U. directive imposes limitations on the transfer of private information beyond member borders unless that country ensures an "adequate level of protection" for such data.[20] U.S. companies doing business in Europe must adhere to the Safe Harbor data protection agreement concluded between the U.S. Department of Commerce and the European Commission in November 2000. The agreement – to which companies must attest that they provide "adequate" privacy protections – enables U.S. companies to avoid interrupting their business dealings with the E.U.[21]

Here is a run-down of various national consumer privacy laws throughout the E.U. and some of the country-specific provisions:

The United Kingdom: a model law

The Data Protection Act 1998, which took effect in March 2000, is a model for national laws enacted throughout Europe. The law grants consumers certain rights while at the same time requires companies to be open about how they use personal information. Companies must abide by eight principles of "good information handling." Those principles are that data must be: fairly and lawfully processed; processed for limited uses; not excessive; accurate; not kept longer than necessary; processed in accordance with consumers' rights; secure; and not transferred to countries without proper protections.[22] The U.K. law also provides for special exceptions for the collection of sensitive information – such as racial or ethnic origin, political opinions, religious beliefs, health, and sex life. These can only be collected if there is specific consent, if required by law, if they are needed to protect the vital interests of the subject, or if they deal with a judicial or legal proceeding.[23] The easiest way for a business to abide by the act is to get consent to gather information directly from the consumer. On 11th December 2003, the Privacy and and Electronic Communications Directive came into force requiring that explicit permission must be given by the consumer, such as the ticking of an 'opt in' box, before marketing material may be sent. This brings the UK in line with other European countries like Germany, whereas previously UK companies could infer consumers' consent to receive promotional literature through their failure to fill in an 'opt-out' box.

[20] Privacy International and the Electronic Privacy Information Center, "Privacy & Human Rights 2003" (http://www.privacyinternational.org/survey/phr2003/)
[21] U.S. Department of Commerce, Safe Harbor, (http://www.export.gov/safeharbor/)
[22] UK Information Commissioner, 1999, "Media Briefing on the New Law" (http://www.dataprotection.gov.uk/media/download/mediasum.pdf)
[23] Ibid

Italian medical data and sensitive information protections

In Italy, the Law n. 675 of 31st December 1996 ("Privacy Act") contains specific regulations requiring companies to attempt to secure data with anti-virus and firewall devices. The law also provides more stringent security rules for maintaining confidentiality of medical data and other sensitive information, similar to the law in the U.K. In order to process sensitive information, notification to the data privacy authority required under the E.U. privacy directive is not enough; companies must receive authorization from the authority to collect such information. In addition to civil, criminal and administrative sanctions for violators, individuals have the right to file suit against the database owner in court.

Selected European Laws	
U.K.	Data Protection Act 1998
Italy	Law n.675 "Privacy Act"
Spain	Act 15/1999
France	Informatique et Libertes
E.U.	Data Protection Directive

Spanish law outlines three levels of confidential data security

The Spanish law protecting data -- Act 15/1999 of December 13 of Protection of Personal Data – sets out three levels of security depending upon the type of data gathered or maintained. The "basic" protection level is applicable to all files containing personal data and mandates that firms create security documents for employees who have access to the data, have procedures in case of a violation, and provide for review when files are modified. The "medium" level covers files containing personal financial information, records of public services, and criminal or administrative records. In order to meet this level of security, an organization must audit the hardware and software programs installed to protect the data confidentiality every two years and keep a registry of all inputs and outputs. The "high" level applies to files containing data regarding political or religious ideologies, race, health, sexual information, and police information. Additional safeguards include the scrambling of any data that is transferred or distributed, a registry of persons who access the files, and monthly reports regarding access to the data.

German law created privacy police to ensure confidentiality

Germany developed some of the toughest privacy laws in Europe following the reunification of the country and the opening of files detailing Soviet-era spying. The former West Germany adopted federal data protection laws as far back as 1977 and revised them in 1990 and again after reunification in 2001. The laws set up an independent Federal Commissioner for Data Protection, who has a staff that polices privacy data compliance in the private and public sectors and requires corporations to have their own data protection officers. The Commissioner for Data Protection enforces laws that give individuals control over their personal data, limiting the ability of companies or governments to collect or maintain personal files.[24] After the E.U. privacy directives were approved, German privacy inspectors traveled all the way from Berlin to Sioux City, S.D., to inspect Citigroup's data-processing center, where it stores financial data on millions of credit card holders worldwide. Citigroup accepted these inspections in return for

[24] Privacy Exchange, legal library, (www.privacyexchange.org)

approval to market credit cards in Germany.[25] With the prospect of on-site visits, companies need to take stringent measures to demonstrate that they have safeguards in place to protect data.

France's pre-existing privacy protection law

Although France has yet to enact a law in response to the E.U. directive, a preexisting law of January 6, 1978 known as "Informatique et libertés" pertains to computers, personal data files, and the rights of citizens. France already has a data protection agency, the Commission Nationale de l'Informatique et des Libertés (CNIL), which records details of data files, creates standards, ensures that consumers can access data files, assess claims, and informs people of their rights. Breach of the law is punishable by up to three years in prison, and a fine of € 45,000, even where committed by negligence.

European protection of business data

Leaks to the media have a galvanizing effect on companies to better protect confidential information. Many European countries have additional laws – some old and some new – providing for the protection of confidential information about companies. The French Labor Code punishes directors or employees of a business who divulge manufacturing secrets with possible sanctions of up to two years in prison and a fine of € 30,000.[26] In the U.K., publicly listed companies are subject to laws and regulations requiring them to disclose financial information if the development may lead to share price movement. The need to protect this type of information from being leaked via e-mail by employees was made crystal clear to companies there in the last few years after the government of Prime Minister Tony Blair was twice embarrassed by its own internal communications. A notorious e-mail from Jo Moore, a special adviser, said that Sept. 11, 2001, would be a good day to bury bad news in the press. In mid-2003, the Blair administration was red-faced by the publication of an internal communication seeking to identify the source of BBC allegations that its records of weapons of mass destruction in Iraq were "sexed up."[27]

Australia: confidentiality laws extend to business

The potential risk for companies that employees will leak confidential information in violation of corporate disclosure laws also was underscored by an Australian case this year. A series of corporate collapses in Australia in 2000 and 2001, such as telecommunications company One.Tel and insurance giant HIH, brought increased attention to corporate governance and the need for transparency among public companies.[28] Changes went into effect in January 2003 to the Corporations Act requiring public disclosure of business information by companies listed on the Australian Stock Exchange (ASX). Companies are now obliged to immediately disclose material information about the business, unless it is confidential or indefinite or no reasonable person would think it would cause a change in the company's value or share price.

---

[25] Business Week, November 2, 1998, " Europe's Privacy Cops" (http://www.businessweek.com/1998/44/b3602159.htm)
[26] Article L. 152-7 of the French Labour Code
[27] The Independent , August 21, 2003, "E-Mail Traffic Reveals the Frenzied Atmosphere of a Mole Hunt" by Andrew Grice
[28] The Sun-Herald, August 11, 2002, "Many.tel of hurt and anger at greed of rich" by Frank Walker (http://www.smh.com.au/articles/2002/08/10/1028158032423.html)

But, already, the Australian Securities and Investments Commission has filed proceedings in federal court alleging that the wine group Southcorp breached the disclosure law as a result of an e-mail that sparked an eight percent drop in the company's share price. On April 18, 2002, Southcorp officials e-mailed an assortment of analysts information about the company's dismal forecast for earnings for the year ending June 30, 2003. The ASIC charged that the information should have been disclosed publicly to the Australian Stock Exchange and wants a court declaration that Southcorp's conduct breached disclosure obligations. Under the Corporations Act, breaches can attract financial penalties of up to $200,000.[29]

In 2000, the Australian government also amended the country's Privacy Act of 1988, which previously spelled out the collection, use, and protection of personal data collected by the government. New provisions that went into effect in December, 2001, mean that privacy principles now apply to the private sector as well.[30] The Act contains a set of National Privacy Principles that detail how businesses should collect, use, secure, and disclose personal information. Special provisions are made for sensitive and health information, as well. The act also requires companies to take "reasonable steps" to protect the personal information it holds from misuse and unauthorized disclosure, listing such technology tools as audit trails, firewalls, network intrusion detection systems, and encryption among other products.[31]

The business case for protecting confidentiality

In addition to the new confidentiality laws enacted around the globe, corporations need to better manage content security for a growing number of other business reasons. A 2001 survey of online consumers in the U.S. found that 63 percent would not buy something from a company online if they had concerns about how their personal data would be used.[32] One third of Britons (32 percent) and Germans (35 percent) have declined to purchase something online because of concerns about the use of private information.[33] New research on Internet and e-mail usage in Australian workplaces found that 22 percent of people have accidentally sent e-mails to the wrong person, and of those, one quarter contained confidential information.[34] In addition to losing business, companies need to better secure data because up to $70 million in proprietary information is lost through cyber crime each year, according to a Computer Security Institute survey.[35] Furthermore, companies consistently had as much to fear from their own employees as from outside hackers.[36] Another growing threat is the risk posed by the unchecked online activities of employees, with companies facing multi-million-dollar liabilities for employees' offensive e-mail, harassment of others, and illegal downloading of copyrighted content. Late last year, the Recording Industry Association of America won a $1 million settlement with Integrated Information Systems, a Tempe, Ariz. company, whose employees had been operating a computer server for music swapping.[37]

---

[29] The Australian Financial Review, February 27, 2003, "Southcorp faces ASIC legal action'" by Simon Evans
[30] Office of the Federal Privacy Commissioner, Federal Privacy Act (http://www.privacy.gov.au/publications/pianew.html)
[31] Ibid
[32] Consumer Privacy Attitudes and Behaviors Survey Wave II, July 2001, Harris Interactive for the Privacy Initiative leadership (http://www.bbbonline.org/UnderstandingPrivacy/library/harris2-execsum.pdf)
[33] IBM Multi-National Privacy Survey Consumer Report, October 1999, Louis Harris & Associates (http://www-1.ibm.com/services/files/privacy_survey_oct991.pdf)
[34] 2003, "SurfControl Internet & Email in the Workplace Survey" by Dr. Monica Whitty
[35] 2003 Computer Crime and Security Survey, Computer Security Institute, www.gocsi.com
[36] Ibid.
[37] Business Week, November 11, 2002, "First Napster…You May be Next" by Lorraine Woellert

Protecting confidential data with SurfControl

In the information economy, safeguarding confidential information by solely human means – such as manual key entry – can be cumbersome, expensive, and subject to inaccuracies. Companies clearly need to seek legal counsel for specific details regarding adherence to some of the new confidentiality laws. But technological solutions can be deployed to help companies secure the large assortment of data flowing in and out of their organizations at a rate expected to exceed 36 billion person-to-person e-mails worldwide by 2005.[38]

Technological solutions can be deployed to help companies secure the large assortment of data flowing in and out of their organizations at a rate expected to exceed 36 billion person-to-person e-mails worldwide by 2005.

Research firm IDC has ranked SurfControl the leader in the growing content security market, which experienced a 49 percent jump in revenues in the past year.[39] One of the main components of the market is messaging security software, which includes e-mail filters and instant message screening applications. Messaging security software can protect a company's intellectual capital, 90 percent of which – from inventions to source code – is in digital format.[40] Of that, 45 percent of those ideas are stored in an organization's e-mail system at any given time.[41] These tools first gained popularity as a means for filtering e-mail for non-legal reasons – to prevent employee productivity problems and to prevent the infection of a company's computer network with an e-mail borne virus. But a growing number of companies are now turning to these tools to also protect a company's reputation from disclosure of customer information and help meet the growing assortment of laws protecting financial, medical, and other sensitive data.

SurfControl's E-mail Filter contains customization tools to allow IT managers to prevent confidential digital information about companies or people from leaving an organization. Using a combination of artificial intelligence, lexical analysis, and technology that can recognize patterns much like the human brain, e-mail is reviewed for select words and word combinations before reaching company mail servers, protecting companies from harmful disclosures. For example, the filtering software can be customized to recognize keyword combinations to help a hospital adhere to HIPAA guidelines by blocking the distribution of files containing patient ID numbers or medical records. The filters also can be customized to recognize a company's quarterly financial reports in order to prevent people from leaking reports before the company formally discloses the information according to the U.S. SEC's Regulation FD or Australia's Corporations Act.

These days, e-mail isn't the only form of electronic communications a company needs to monitor and control. Use of public instant messaging and peer-to-peer networks to exchange content have emerged as a growing threat to confidential information and compliance with regulations. These tools, once purely for entertainment, have rapidly infiltrated corporate networks with a vengeance. SurfControl's Instant Message Filter allows companies to block public IM traffic or peer-to-peer applications entirely, permit usage of only certain products, or restrict the use of these tools to certain employees or departments.

---

[38] Agence France Presse, Sept. 17, 2001, "E-mail to more than double: study"
[39] IDC, July 2003, "Content Security: The Business Value of Blocking Unwanted Content" by Brian E. Burke
[40] SC Magazine, August 2001
[41] SC Magazine, August 2001

Around the globe, governments are responding to the rapid spread of Internet and e-mail use in the workplace with new laws and regulations that protect the flow of confidential consumer and business information. Businesses need to evaluate the cost savings and ease with which they can comply with these new laws by using messaging security software to supplement – and sometimes replace – the more costly human monitoring solutions. With a thoughtful approach, involving risk assessment, development of company policies and deployment of technological solutions, companies can best meet the new legal mandates governing the care and handling of confidential information.

About SurfControl

SurfControl plc, the world's number one Web and e-mail filtering company, delivers on its promise to help companies 'Stop Unwanted Content' in the workplace by continuous innovation, invention and expansion of its filtering products to address new content risks as they emerge. The company is the leader in the Content Security market which analysts expect to reach nearly $2 billion by 2007.

SurfControl is the only company in the security market offering a total content security solution that combines Web, E-mail (including Anti-Spam and Anti-Virus) and Instant Message Filters with the industry's largest, most accurate and relevant content database and adaptive reasoning tools to automate content recognition.

SurfControl's world-class partners include Sun Microsystems, Check Point, Cisco, IBM, Research In Motion and Nokia. The company has more than 20,000 customers worldwide, including many of the world's largest corporations, and employs nearly 450 people in nine separate locations across the United States, Europe, and Asia/Pacific.

About Hammonds

Hammonds [www.hammonds.com], one of Europe's largest commercial law firms, provided SurfControl with information on U.K. and European law relating to the protection of confidential information.

For more information about SurfControl content filtering solutions, or to download a free trial of SurfControl Web, E-mail or Instant Message Filter, visit www.surfcontrol.com