Global Co-Operation in the New Millennium
The 9th European Conference on Information Systems
Bled, Slovenia, June 27-29, 2001

CYBERLIABILITY: IS THE CHIEF PRIVACY OFFICER THE SOLUTION?

Janice C. Sipior

Villanova University, Villanova PA 19073 USA
Tel.: 1 610 519 4347, Fax: 1 610 519 5015
janice.sipior@villanov.edu

Burke T. Ward

Villanova University, Villanova PA 19073 USA
Tel.: 1 610 519 4375, Fax: 1 610 519 5204
burke.ward@villanova.edu

ABSTRACT

The primary responsibility of the Chief Privacy Officer (CPO) is to protect online consumer privacy by developing an organization's privacy policy and ensuring compliance with privacy laws and regulations. However, the explosive growth of internet use for business has brought about an escalation of concerns including reduced consumer confidence in internet-related business activities, risk of financial loss, and legal liability from sources categorized as external and internal to the organization. Does the new CPO position provide adequate consideration of the increasing risks? This paper discusses the far-reaching types of misconduct and risks organizations face. The paper concludes by recommending an expanded role for the CPO. In addition to overseeing internet privacy issues, the new role of Chief Privacy and Integrity Officer (CPIO) would encompass internet integrity. This entails formulating or reformulating an expressed internet use policy, undertaking on-going training and other means to maintain awareness of issues, monitoring internal sources, implementing defenses against external sources, and securing adequate liability insurance. The effectiveness of this new role, in overseeing these responsibilities, would be determined by assessing current operations, implementing proactive measures to reduce potential misuse, and continuously keeping abreast of technological advances, legislative and regulatory initiatives, and new areas of vulnerability.

1. INTRODUCTION

Internet access continues to expand, with current estimates ranging from 130 million (Nielsen, 2000) to 304 million internet users worldwide (Nua, 2000). There are an estimated 46.5 million users in the United States (US) alone, expected to reach 90 million in the next four years (Strategis Group, 2000). The explosive growth of internet use for information access, file transfer, email, collaborative work, banking, shopping, and performing countless other functions has brought about an escalation of concerns. The advantages of quick access to timely data and less restricted communications resulting from internet connectivity have been

accompanied by reduced consumer confidence in internet-related business activities, the risks of financial loss, and legal liability from sources both external and internal to the organization.

Most recently, organizations have responded by creating the position of Chief Privacy Officer (CPO). Current estimates place the number of CPOs at no more than 50 – 75 in the US. This number is expected to increase into the thousands, as companies discover "that their ability to manage privacy is a major part of their competitive edge" (Thibodeau, 2000). The primary responsibility of the CPO is to protect online consumer privacy by developing the organization's privacy policy and ensuring compliance with privacy laws and regulations. The creation of this position is largely in response to new privacy related laws and regulations. For example, three significant new laws and regulations imposing privacy standards in the US went into effect November 1, 2000. Included among these are the Gramm-Leach-Bliley Financial Modernization Act directed at consumer privacy in the financial services industry, the Health Insurance Portability and Accountability Act which ensures patients' medical records are private, and the U.S. Department of Commerce's safe harbor list intended to assist U.S. company's compliance with the European Union Data Protection Directive. While appropriate for issues of consumer privacy, does the new CPO position provide adequate consideration of the increasing risks facing online organizations?

The first line of defense in responding to increasing risks resulting from inappropriate internet activities is to raise the awareness and understanding of what the risks are and how they might arise. This paper first discusses the various types of misconduct and the risks organizations face. The scope of considerations is far-reaching. Certainly, this discussion is not comprehensive. Any effort to address all possible threats is never-ending, as online activities are limited only by the imaginations of an increasingly internet savvy workforce and worldwide population. The paper concludes by recommending an expanded role for the CPO. In addition to overseeing an organization's internet privacy issues, the role of CPO should encompass internet integrity. Thus, this individual's realm of responsibility would encompass not only privacy related laws and regulations, but also online content liability and the interpretation of laws and regulations as applied to the internet.

2. ORGANIZATIONAL RISKS OF INTERNET USE IN BUSINESS

To promote an understanding of the types of misconduct and the risks to which organizations are subject, this section presents example instances of threats to internet use in business. As shown in Figure 1, the sources of these threats are categorized as external, both external and internal, and internal to an organization. Each of these categories is not exclusive, but rather there is overlap among them. The purpose of the categorization is to reveal the motivation and implications resulting from each source. A summary of the sources and corresponding threats are presented in Table 1.

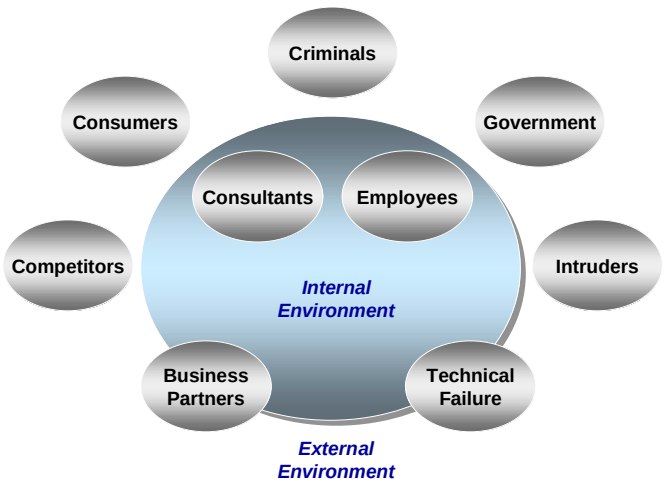

Figure 1: *Sources of threats to internet content and use in business*

External sources	Both External & Internal	Internal sources
Competitors	**Business partners**	**Employees & Consultants**
• Copyright infringement	• Global trade violations	• Employer Liability:
• Intellectual property loss	• Cookie sharing	o Copyright infringement
• Trade secret loss	**Technical failings**	o Defamation & Libel
Consumers	• Device defects	o Discrimination
• Invasion of privacy	• Loss of network	o Harassment
Criminals	• Misdelivery	o Hostile work environment
• Defaced websites	• Password loopholes	o Obscenity
• DDoS attacks		o Pornography
• Hacking & Cracking		o Invasion of privacy
• Malicious code		o Securities violations
• Theft		o Trademark & Trade secret violations
Government		• Loss of employee productivity
• Discovery (supeona)		
• Law enforcement (search warrant)		
Intruders		
• Cookies		
• Spam		

Table 1: *Sources and example threats to internet content and use in business*

2.1. External Threats to Online Organizations

Online organizations are subject to a diversity of challengers from the external environment. Each of these sources may have differing motives, but may nonetheless cause financial loss or reduced confidence in internet-related business activities of the targeted organization.

2.1.1 Competitors

Competitors and industry spies may seek to gain access to copyrights, intellectual property, trade secrets, and other proprietary information. Intelligence gathering has occurred for decades, including traditional spying methods such as browsing at a competitor's store, posing as a customer, searching obscure public records, or counting deliveries at the loading dock. In what Microsoft Corp. called a deplorable act of corporate espionage, hackers gained access to its computer network by using an email account in Russia to steal passwords to the network. At a minimum, the hackers were able to view source code to recent versions of

the Windows operating system and portions of its Office suite. Organizations must be on the alert to recognize the corresponding e-methods for spying.

2.1.2. Consumers

The major concern of consumers focuses on privacy. Online businesses have increasingly sought to tailor website interaction and target promotional activities to individual consumers. This requires the collection of various types of data, preferably identified with a specific individual.

The use of cookies enables personal information to be easily obtained from web users, often without their knowledge. In addition to click-stream data, cookies can collect the user's IP address, the number and dates of prior visits, the type and version of browser and operating system, among other types of information. Further, users may be asked to provide registration information when visiting a website which, when combined with data collected through tracking technology, can be used to create an individual user profile. Subsequently, this information may be used to send unsolicited bulk e-mail, or spam. While primarily utilized for commercial purposes, spam may also promote political, malicious, or illegal schemes.

Consumer reaction has ranged from outrage to filing lawsuits against major internet companies for failure to disclose data collection practices or to comply with their own published privacy policy. Among the companies named in claims are Amazon.com, DoubleClick, RealNetworks, and Yahoo!. In addition to the special regulations which recently went into effect, the Federal Trade Commission recently asserted its authority by bringing enforcement actions against websites for questionable data collection practices.

2.1.3 Criminals: Hackers and Crackers

Legal commentators are divided over how internet crime, or cybercrime, should be addressed (Sinrod and Reilly, 2000). Cybercrime can either be viewed as traditional crime committed with computer resources or as a new category with unique considerations requiring a new legal framework. Emerging technologies are accompanied by emerging challenges such as perpetrator identification, intent and motivation, jurisdiction, and international cooperation. Although acting from outside of an organization, disgruntled insiders are the primary perpetrators of internet crimes (Cherry, 2000). The perpetrators are generally referred to as hackers or crackers have cost U.S. businesses an estimated US$10 billion annually, according to the FBI (Goch, 2000), from various activities ranging from simple criminal trespass to sophisticated website defacing, distributed denial of service (DDoS) attacks, hacking and cracking, malicious code, and theft of proprietary information, resources, and services.

Website defacing entails unauthorized access to either a user's account or the webmaster's password to download, alter, and upload a webpage. Perhaps the most brazen of website defacing was directed against the Federal Bureau of Investigation which investigates this criminal violation of federal law.

DDoS attacks direct numerous computers to send service requests to a targeted website. A rash of DDoS attacks against prominent websites, including Amazon.com, eBay, and Yahoo!, occurred in February 2000. The servers at these targeted sites were so overwhelmed that the sites were unable to respond to legitimate requests, causing more than US$1.2 billion in total losses (Banham, 2000). The estimated losses are based on each company's lost revenues for site down time, lost market capitalization due to plunging stock prices, and the cost for systems security upgrades. Future losses may result from a reduction of consumer confidence in e-commerce. Additionally, organizations and Internet Service Providers could be held liable for unwittingly allowing their computers to partake in the attacks, according to an industry consortium set up to fight threat of DDoS (Greene, 2000).

Hacking and cracking entails trespass for the challenge or thrill of gaining illegal entry, illicit financial gain, or malicious activities. According to a survey by the FBI, 55% of respondents reported malicious activity by disgruntled insiders (Vatis, 2000). A former employee of Forbes, Inc. used a co-worker's account to vengefully cause five network servers to crash and erased the server volume on each. A two day shut down

of Forbes New York operations resulted in losses exceeding US$100,000.

Malicious code is devised to cause damage or to steal information. There are an estimated 30,000 viruses in existence, with approximately 300 new viruses created each month (Sinrod and Reilly, 2000). The most common forms are viruses, worms, and Trojan programs, designed to spread from one computer to others via executable code in email or infected disks. The resulting damage can be quite costly, with the Melissa Macro Virus causing an estimated US$80 million and the "ILOVEYOU" virus an estimated US$10 billion in damage worldwide (Goch, 2000).

2.1.4 Government

The government may gain access to internet content through law enforcement activities or discovery processes. Law enforcement agencies investigating illegal activities may present a search warrant to search files or e-mail messages in transit, stored on disk or in paper form, backed-up to tape, or even those which have been deleted and overwritten. Similarly, through discovery, a supeona may be issued. For example, email messages written by Bill Gates were retrieved and used as evidence to support the Department of Justice's antitrust lawsuit alleging that Microsoft used its Windows monopoly to unfairly crush Netscape Navigator. Antitrust experts commented that the messages constituted some of the most damaging evidence against Microsoft.

2.1.5 Intruders

Organizations are subject to intrusions for activities which are not illegal, but may certainly be disruptive. Unlike criminals who gain illegal unauthorized entry, marketers and advertisers are able to intrude upon the privacy of employees through cookies and spam. Organizations may question the methods and types of information collection and the use of that information. Further, spam can overload a company's server and cause it to slow or crash.

2.2 Both External and Internal Threats to Online Organizations

Threats to internet content may straddle the external and internal environment through sources such as business partners and technological failings. Business partnering may include formal and informal alliances established for a joint project. Technological glitches can expose organizational content to perusal by unintended sources.

2.2.1 Business Partners

Organizations are less likely to view business partners as a threat, in contrast to other sources such as competitors. However, the interests of a partner organization lie primarily with furthering its own goals. An organization may be liable not only for the actions of its own employees, but also for those of partner employees. The risks from a source which is both external and internal can become more complicated.

Global partnering, for example, requires compliance with a multitude of trade laws worldwide. Websites must comply with the European Union's privacy laws, which restrict the collection of personal data. Other areas of global restrictions include consumer protection laws, advertising restrictions and the international equivalents of the U.S. Food and Drug Administration.

A risk unique to website partnering is cookie sharing, the practice of collecting and consolidating information gathered from various websites. Another form of cookie sharing is achieved by multiple cookie creators partnering to share one website. Cookies can be sent to a user from a domain other than the site the user visited. For example, an advertising agency could post its clients' banner ads from a central server and include cookies to track the activities of users receiving the ad. The user is unlikely to know what site created the cookie, and therefore less likely to know the intended use of the user profile obtained.

2.2.2 Technical Failings

Internet content may be at risk due to technical failings including device defects, loss of network integrity and availability, misdelivery of email messages or files, and password protection loopholes. In managing resources, an internal system administrator can for example, monitor employees' email, as was the case at Epson America, Inc. (Sipior and Ward, 1999), or files. This interception was by an internal employee, but the content examined could be outside of the employee's realm of responsibility. Similarly, an ISP can intercept communications without liability as long as it is necessary to provide services or to protect property, again relinquishing content, but this time to someone external to the organization. Message delivery misdirection resulting from a technical glitch may also reveal content to unintended recipients.

2.3 Internal Threats to Online Organizations

Those within an organization, including consultants and employees, may inadvertently or intentionally cause their employer shared liability for their actions. The most common concerns for liability on the internet are copyright infringement, pornography, and defamation (Goldstein, 2000). We consider a wider array including copyright infringement; defamation and libel; discrimination, harassment, hostile work environment, obscenity, and pornography; invasion of privacy; violations of securities laws; and violations of trademark and trade secret laws. Although these areas illustrate potential liability on the part of employers for employee internet activities in the workplace, the legal precedents regulating this arena are still evolving (Rosove, 1997).

2.3.1. Copyright Infringement

The copyright laws of the U.S., intended to balance the rights of users and creators, include protection of the various materials found on the internet (Copyright Act, 1994). The ease with which electronic material can be copied has resulted in a rapid increase in copyright infringement on the internet. Copyright infringement committed by an employee may result in employer liability, even if the employer did not perform the copying or distributing.

Employer liability can result from what may seem to be innocent activities. An employee may have brought in an individually licensed copy of software from home, copied software from the web, or cut and pasted clipart from other websites. For example, the webmaster of the National Association of Fire Equipment Distributors used copyrighted clipart, obtained from three CD-ROM volumes, to decorate the trade organization's website. In the ensuing lawsuit, Marobie- Fl. Inc. d/b/a Galactic Software v. National Association of Fire Equipment Distributors et al. (2000), the trade organization was held liable for copyright infringement. The bottom line is that if an employer has possession of improperly obtained materials for which valid purchase receipts cannot be provided, it may be charged with copyright infringement.

2.3.2. Defamation and Libel

The various forms of internet communication have given rise to employee cybersmearing or cyberventing, the virtual equivalent of casual conversations around the water cooler. Unwitting or disgruntled employees have utilized bulletin boards, chat rooms, email, and websites to anonymously vent opinions, concerns, frustration, or anger about the workplace. For most large companies, at least one website is available while for others, such as Microsoft, there are several.

The common law tort of defamation is intended to protect an individual's interest in his own reputation. Defamation can be difficult to prove for a public company. Postings must contain false statements, not just an opinion, be made knowingly and recklessly, and hurt the company. In what has been described as a case of cyberventing gone too far, a former engineer of Intel Corp. created a website as a critical forum for a group called Former and Current Employees of Intel (Apsen Law & Business, 1999). Intel has not filed a

defamation charge for the site. Rather, a restraining order was placed against the former employee in response to unsolicited mass emails sent to as many as 30,000 Intel employees. Intel chose to effectively cease the offender's activities rather than pursue a lengthy case, drawing more attention to that which they sought to stop.

Frequently, the intent of a lawsuit is not about defamation, but rather to reveal the names of anonymous detractors. For example, the Raytheon Co. suspected postings to a Yahoo! Finance message board were made by an employee (Associated Press, 1999). In the ensuing lawsuit, Raytheon obtained subpoenas against Yahoo! and other internet services to learn the identity of all 21 aliases, most of whom were employees, and then dismissed the suit. Four employees subsequently resigned; others entered corporate counseling.

2.3.3. Discrimination, Harassment, Hostile Work Environment, Obscenity, and Pornography

According to the Communications Decency Act of 1996, employers are not liable for obscene or harassing use of electronic telecommunications by their employees unless the conduct is within the scope of employment and the employer (1) had knowledge of, and authorized, the conduct or (2) recklessly disregarded the conduct (CDA, 1998). Under harassment law, an employee may sue for damages based on a "hostile environment," a vague term including an array of offensive elements, such as jokes, chat, pinups, images, and even co-workers gathered around a screen making sexist or racially insensitive remarks.

Unfortunately, instances of such internet abuse abound in the workplace. For example, two African-American employees of Morgan Stanley Dean Witter filed a US$36 million class action suit, later settled, claiming they suffered emotional and physical stress from email messages containing racist jokes (Tran, 1998). Four female employees received a settlement of US$2.2 million from Chevron Corporation for sexually harassing email (Sipior and Ward, 1999). Compaq Computer Corp. fired 20 employees after they downloaded sexually explicit images from websites, logging over 1,000 hits apiece, and distributed the images via email (Bedell, 2000). The New York Times Co. fired 23 employees for distributing pornographic images through e-mail (Rosove, 1997).

2.3.4. Invasion of Employee Privacy

Employers bear the responsibility for managing organizational resources appropriately. In response, increasing numbers of organizations are monitoring internet activities. Among the reasons for monitoring are reduced employee productivity, decreased bandwidth, corporate espionage, and legal liability. Nearly three-quarters of major U.S. companies responding to a survey review some form of their employees' communications including internet connections, email, computer files, or telephone calls (American Management Association, 2000). Of all surveillance methods, internet and email monitoring have seen the most explosive growth, with 54.1% of companies now monitoring employees' internet connections and 38.1% reviewing e-mail messages. However, these actions may conflict with legitimate employee privacy expectations in the workplace.

2.3.5. Violations of Securities Laws

A number of provisions of the Securities Exchange Act (SEC) of 1934 arguably prohibit the manipulation of stock prices through false or misleading internet communications. The SEC has taken action in cases of phony internet message board postings. One incident was perpetrated anonymously by an employee of a publicly traded company, PairGain, targeted in his hyperlink posted to a Yahoo! Finance message board (Broersma and Barrett, 1999). The link, which stated, "BUYOUT NEWS!!! ECILF is buying PAIR… Just found it on Bloomberg…" presented an authentic looking spoof of Bloomberg L.P.'s news site. The stock price of PairGain rose nearly 31% before the markets settled. PairGain cooperated fully during the investigation and was never implicated. Nonetheless, the company was subjected to the disruption of the investigation and was undoubtedly concerned about potential liabilities.

Additional concerns include inaccurate disclosures made unwittingly by employees of public companies participating in internet based discussions. Such statements, albeit inadvertent, violate the general antifraud provisions of the Securities Exchange Act (SEC, 1934).

2.3.6. Violations of Trademark and Trade Secret Laws

Similar to copyright infringement, employers may also be held liable for its employee's violations of trademark and trade secret laws. If an employee were to post the trademark of another organization on his employer's website and, when informed, the employer did not take action to correct the infringement, the employer may be held liable. The same rationale applies to an employee's misuse of trade secrets. If an employee used the employer's resources to obtain another organization's proprietary information, such as a customer list or software code, the employer may be liable.

2.4. Loss of Employee Productivity and Internet Resource Use

For some companies, the concern is not what their employees are doing on the internet, but rather the time they spend. For example, at Xerox-PARC, 40 employees were fired for spending as much as eight hours a day visiting inappropriate websites (Bedell, 2000). Ernst & Young reported some firms calculated that more than 80 percent of their internet capacity was used to access non-business related websites (Bedell, 2000). To gain insight into workplace surfing, a survey revealed only 9.6% of respondents never surf non-work related sites, while 12.6% admitted surfing over 2 hours (Vault.com, 2000). Employee web surfing can represent lost productivity, especially when coupled with non-work related emails. About half (51.5%) of respondents to the same survey reported receiving 1-5 non-work related e-mails, on average, during the workday (Vault.com, 2000). Over half (56.3%) send 1-5 emails. Together, these activities could represent an estimated cost of US$9,600 per employee per year, as shown in Table 2 (Dean and Carey, 2000).

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	US$40
Annual cost of lost productivity per employee	US$9,600

Table 2. *Potential losses resulting from decreased employee productivity*
Source: Dean and Carey, 2000.

3. RECOMMENDATIONS: THE EXPANDED ROLE OF CHIEF PRIVACY & INTEGRITY OFFICER

It is evident that as more people gain access to the internet, the numerous potential cyberliabilities confronting online organizations will continue to increase. The burden of repercussions from misuse is placed squarely on organizations, which hold the ultimate responsibility for use of organizational resources by their employees. Interestingly, liability may even extend to inadequate site security resulting in unwitting participation in internet abuses such as DDoS attacks, as previously discussed.

In response, organizations may place the responsibility of overseeing internet activity on the existing legal department or on one or more chosen individuals, depending on the size and resources of the organization. In order to effectively coordinate proactive and reactive organization-wide action to potential consequences, we recommend expanding the role of the existing CPO to include internet integrity. Responsibilities would

be expanded from focusing on consumer privacy to ensuring the integrity of both internet content, including websites, files, email, and communications, and internet use, including the direct activities of internal sources and the consequences of external sources. Thus, this emergent role would more appropriately be titled Chief Privacy and Integrity Officer (CPIO) to protect organizational resources while maximizing the use of the internet. Certainly this expanded set of responsibilities should be accompanied by an expanded set of qualifications. A legal specialization in consumer privacy would be necessary to assure organizational adherence to government regulations, industry self-regulation, and organizational initiatives associated with consumer privacy. Proactively attending to the broad spectrum of internet activities and potential unintended consequences requires both an expanded legal background, including online content liability and the interpretation of laws and regulations as applied to the internet, and an extensive technical understanding to minimize the occurrence of threatening internet activities.

Specifically, the newly defined CPIO would be responsible for formulating or reformulating an expressed internet use policy, undertaking on-going training and other means to maintain awareness of issues, monitoring internal sources, implementing defenses against external sources, and securing adequate liability insurance. The effectiveness of this new role, in overseeing these responsibilities, would be determined by assessing current operations, implementing proactive measures to reduce potential misuse, and continuously keeping abreast of technological advances, legislative and regulatory initiatives, and new areas of vulnerability.

3.1. Internet Use Policy

The internet use policy should clearly state what is acceptable and unacceptable use of specific internet technologies, by whom, at what times, for what duration, and for what purposes (Whitman, 1999). Details about personal use, prohibited use, and access to prohibited materials should be comprehensively stated. Privacy rights, if any, for allowable personal use should be defined to clarify employee expectations. The various types of use prohibited under all circumstances should be enumerated, such as is criminal, disruptive, offensive, harassing, or otherwise unethical use. Access to prohibited materials such as that which is copyrighted, licensed, other intellectual property, sensitive company materials, or otherwise illegal should be explicitly condemned. Procedures for identifying violations must be communicated. The consequences of policy violations should be stated.

3.2 Training

The development of a formal internet use policy can promote improved use, especially if reinforced by communicating that policy, and conducting education, training and re-training sessions. Other means to maintain awareness of issues may be employed, such as presenting the internet use policy each time an employee logs-in or presenting a pop-up reminder when certain system facilities are accessed. Employee awareness of appropriate internet use could thereby be kept up-to-date, even as technological advances and associated new means of abuse occur.

3.3 Monitoring Internal Sources

Since it is the employer who is held responsible for employee abuse of the internet, monitoring or reserving the right to monitor is a necessary means to appropriately manage resources. Generally, U.S. federal law allows employee monitoring for business purposes if the employees have been made aware of the extent of monitoring. However, in implementing monitoring programs, applicable statutory, regulatory, and common law requirements intended to protect employees' privacy interests must be considered. If undertaken, such monitoring may reveal the need for filtering software to block employee access to inappropriate websites, chat rooms, message boards, and Usenet news groups.

3.4 Defenses Against External Sources

Automated defenses should be employed against external sources, such as intrusion detection systems, firewalls, virus protection programs, security patches for operating systems, and encryption and authentication products. Procedures to update these defenses should be established to minimize the adverse effect of technological advances rendering current versions obsolete.

3.5 Liability Insurance

Organizations may reduce financial exposure of liability by purchasing insurance. Among the most costly and common risks to online organizations are business interruptions caused by hackers, viruses, and internal saboteurs; litigation costs and settlements for inappropriate employee e-mail and internet use; failure of products or services to perform as advertised on the internet; copyright and trademark lawsuits; and patent-infringement claims (Goch, 2000). The insurance industry has responded by providing various products directed toward e-business.

REFERENCES

Apsen Law & Business (1999). Superior Court Enjoins Sending of Unsolicited Emails by Former Employee. *Computer Lawyer*, January, 16 (1).

American Management Association (2000). A 2000 AMA Survey: Workplace Testing, Monitoring, and Surveillance. http://www.amanet.org/research/pdfs/monitr_surv.pdf

Associated Press (1999). Raytheon Drops Suit Over Internet Chat, *The N.Y. Times On The Web*, May 22, http://www.nytimes.com/library/tech/99/05/biztech/articles/22raytheon.html

Banham, R. (2000). Hacking It. *CFO, The Magazine for Senior Financial Executives*, August 1, 2000, 16 (9), WL 15330559.

Bedell, D. (2000). Access vs. excess: Employers cracking down on illicit Web surfing in workplace. *The Dallas Morning News*, March 12, WL 14659363.

Broersma, M. and L. Barrett (1999). Bogus Report Boosts Internet Stock, *ZDNet News Tech News Now - Business*, April 7, http://www.zdnet.com/zdnn/stories/news/0,4586,2238191,00.html

Cherry, S. R. (2000). Computer Hacker Sneak Attacks. *Insight Magazine*, 16 (11), WL 22984041.

Communications Decency Act (CDA) of 1996, 47 U.S.C. §223 (e) (4) (1998).

Copyright Act, 17 U.S.C. § 102 (1994) (defining copyrightable subject matter).

Dean, R. and A. Carey (2000). Executive Insights on Content Security, International Data Corporation, http://www.idc.com

Goch, L. (2000). Survey Shows U.S. Businesses Lack E-Risk Coverage. *Best's Insurance News*, July 28.

Goldstein, M.P. (2000). Service Provider Liability For Acts Committed By Users: What You Don't Know Can Hurt You. *John Marshall Journal of Computer and Information Law*, Spring 2000

Greene, T. (2000). Forum warns of hidden DDoS legal liability. *Network World*, October 2, WL 9436519.

Marobie- Fl. Inc. d/b/a Galactic Software v. National Association of Fire Equipment Distributors et al., No. 96-C-2966 (N.D. Ill., July 31, 2000).

Nielsen NetRatings (2000). http://209.249.142.29/nnpm/owa/Nrpublicreports.usagemonthly

Nua Internet Surveys (2000). http://www.nua.ie/surveys/how_many_online/index.html

Rosove, S. (1997). Employee Internet Use. *New York Law Journal*, March 17, http://ljx.com/practice/laboremployment/0317empl.html

Securities Exchange Act of 1934.

Sinrod E.J. and W. P. Reilly (2000). Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws. *Santa Clara Computer and High Technology Law Journal*, May.

Sipior, J.C. and B.T. Ward (1999). The Dark Side of Employee E-mail. *Communications of the ACM*, 7(7), July, 88-95.

Strategis Group (2000). http://www.strategisgroup.com/press/pubs/intdbl.html

Tran, M. (1998). Wall St Sacks Two in Email Porn Clean-Up. *The Guardian*, April 1, WL 3086937.

Thibodeau, P. (2000). Chief privacy officers emerging in response to data-privacy concerns. *Computerworld*, September 14.

Vatis, M.A. (2000). Internet Security. *Congressional Testimony by Federal Document Clearing House*, March 7.

Vault.com (2000). Results of Vault.com Survey of Internet Use in the Workplace. http://vault.com/vstore/SurveyResults/InternetUse/index2000.cfm

Whitman, M.E., A.M. Townsend, R.J. Aalberts (1999). Considerations for an Effective Telecommunications-use Policy. *Communications of the ACM*, June, 42 (6), WL 9983082.