Chapter XXIII
Electronic Risk Management

Tapen Sinha
Instituto Tecnológico Autónomo de México, Mexico
University of Nottingham, UK

Bradly Condon
Instituto Tecnológico Autónomo de México, Mexico
Bond University, Australia

ABSTRACT

Doing business on the Internet has many opportunities along with many risks. This chapter focuses on a series of risks of legal liability arising from e-mail and Internet activities that are a common part of many e-businesses. Some of the laws governing these electronic activities are new and especially designed for the electronic age, while others are more traditional laws whose application to electronic activities is the novelty. E-business not only exposes companies to new types of liability risk, but also increases the potential number of claims and the complexity of dealing with those claims. The international nature of the Internet, together with a lack of uniformity of laws governing the same activities in different countries, means that companies need to proceed with caution.

INTRODUCTION

Within 48 hours after Katrina came ashore, a number of Web sites cropped up claiming that they are for hurricane relief. At the click of a computer Web site, you could donate money for the victims. Some of them even allowed you to donate money through a Red Cross Web site. Unfortunately, many of them turned out to be fraudulent. When you thought you were going to the Red Cross Web site, you would be taken to a different one and your credit card information would be stolen and sold to the highest bidder. In the electronic parlance, this process is called "phishing" (see Appendix for terminologies).

Electronic information transfer has become the backbone of our information society. Therefore, it is not surprising that it has also increased the

risks coming from electronic sources. The main risk comes from the Internet. For many businesses, and for many individuals, the benefits of being connected to the Internet have increased so much that not being connected to the Internet is no longer an option.

Companies who conduct transactions over electronic channels face a number of risks. Some of these risks, such as viruses, flow from the nature of modern technology. Others, such as theft, are age-old risks that have taken on new twists in the electronic age. For example, banks transfer huge amounts of money by wire, making them easy and lucrative targets for fraud, extortion, and theft. Other financial institutions, such as credit card companies, are prone to the same hazards. Software companies sell their products in electronic format. Copying files and programs is easy and cheap, making software companies particularly vulnerable to theft of their products. Electronic retailers that do all of their business online, such as Amazon.com, are subject to a wide array electronic risks associated with electronic money transfers and Web sites. However, even bricks and mortar companies face numerous risks emanating from (electronic) viruses, hackers, and the online activities of employees. These legal and technological risks associated with e-business—which may be referred to collectively as electronic or cyber risks—are the subject of this chapter.

The aim of this chapter is to survey a broad array of electronic risks that can cause their victims to lose money. It is beyond the scope of this chapter to provide advice on how to manage each and every one of these risks. Rather, this chapter seeks to raise awareness of a variety of risks so that readers will become conscious of the need to develop electronic risk management strategies. The best advice in this regard is to invest in expert advice. For example, where litigation risk exists, consult a lawyer early on regarding strategies to adopt that will avoid litigation or minimize the cost and risk of litigation should it become unavoidable. Where loose lips increase risks, develop strategies for managing the content of correspondence, whether traditional or electronic, such as educating and monitoring employees. Where the problem is primarily a technical one, invest in the necessary technology and expertise. Finally, where insurance is available to manage the financial risks associated with doing business electronically, buy it.

A GLOBAL PROBLEM OF VIRUSES

Computer viruses have become synonymous with electronic risk on a global scale. The method of electronic infection has changed dramatically. In 1996, e-mail attachments were responsible for 9% of infections whereas 57% of infections came from floppy disks. In 2000, 87% infections came from e-mail attachments and only 6% came from floppy disks. By 2004, the rate of infections from e-mail attachments had topped 99% of total infections (Source: ICSA Labs Virus Prevalence Survey, various years). As a result, in 1997, only 30% of all institutions used virus protection for e-mails whereas by 2004, the use of virus protection had almost reached universality (ICSA Labs Virus Prevalence Survey 2004, Figure 15). However, the rise of the use of virus protection has not reduced the rate of infection. Figure 1 shows how the rate of infection has changed over a period of 9 years. Despite the near universal use of antivirus software, the rate of infection has increased more than eleven-fold. The biggest jump in infection came between 1998 and 1999. It has not decreased since (see Table 1).

The number of problems and the associated cost of computer viruses have gone up steadily over the past decade. DARPA created the Computer Emergency Response Team Coordination Center (CERT/CC) in November 1988 after the computer worm Morris worm struck. It is a major coordination center dealing with Internet security problems run by the Software Engineering Institute (SEI) at Carnegie Mellon University.

Table 1. Computer infection rates 1996-2004 (Source: ICSALabs.com)

Infection Rates	Per 1000 Computers
1996	10
1997	21
1998	32
1999	80
2000	90
2001	103
2002	105
2003	108
2004	116

Table 2. Number of incidents reported by CERT 1995-2003 (Source: http://www.cert.org)

Year	No. of Incidents
1995	2,412
1996	2,573
1997	2,134
1998	3,374
1999	9,859
2000	21,756
2001	52,658
2002	82,094
2003	137,529

Note: A CERT "incident" may involve one, hundreds, or thousands of sites. Some incidents may involve ongoing activity for long periods of time.

CERT/CC has compiled a comprehensive list of security "incidents" that have occurred since 1995 (see Table 2). The trend is showing an exponential rise of such incidents over time.

How much do such viruses cost the world? Estimates are available for 1995-2003. It shows that the cost went up quite rapidly between 1995 and 2000, but then there was no clear increase over time. One reason for such a recent slowdown is the widespread use of antivirus programs implemented by businesses as well as individuals.

The damage caused by computer viruses is not uniform across all viruses. A few viruses (and their variants) cause most of the damage. The undisputed world champion was a virus codenamed ILOVEU (see Table 4). It was created by a person in the Philippines. Yet, the most damage it caused was in the developed world. It propagated during the weekend of February 2000 around St. Valentine's Day. The biggest recent attack, in August 2005, was caused by a worm code named Zotob. It took out the computer system of CNN live. It spread through the entire Internet over the weekend. Within 2 weeks, the police in Morocco arrested an 18-year old as the main coder of the worm at the request of the Federal Bureau of Investigation. However, given that there is no extradition treaty in these matter between the United States and Morocco, it is highly unlikely that the person would be extradited to the United States.

THE SPAM-VIRUS NEXUS

Being connected to the rest of the world through the Internet in general, and through e-mails in particular, has a cost. The cost comes in the form of spam. Spam is unsolicited e-mail. The problem of spam has become extremely large. In July 2004, spam accounted for more than 95% of all e-mails (see Figure 1). MessageLabs published a report in 2004 in which it noted that "more than 80% of global spam originates from fewer than 200 known spammers in the USA. Many are based in the small town of Boca Raton in Florida, one of three states in the U.S. which have no spam legislation in place" (Source: http://www.MessageLabs.com). In addition to being a nuisance, spam also represents a big source of electronic risk. Among the devastating viruses, SoBig.F (see Table 4) spread mainly through spam. Thus, spam can not only be a nuisance by itself, but can also carry a payload of viruses.

Figure 1 suggests that some electronic risks can be diminished with adequate legal protection.

Table 3. Annual financial impact of major virus attacks 1995-2003 (Source: http://www.computereconomics.com)

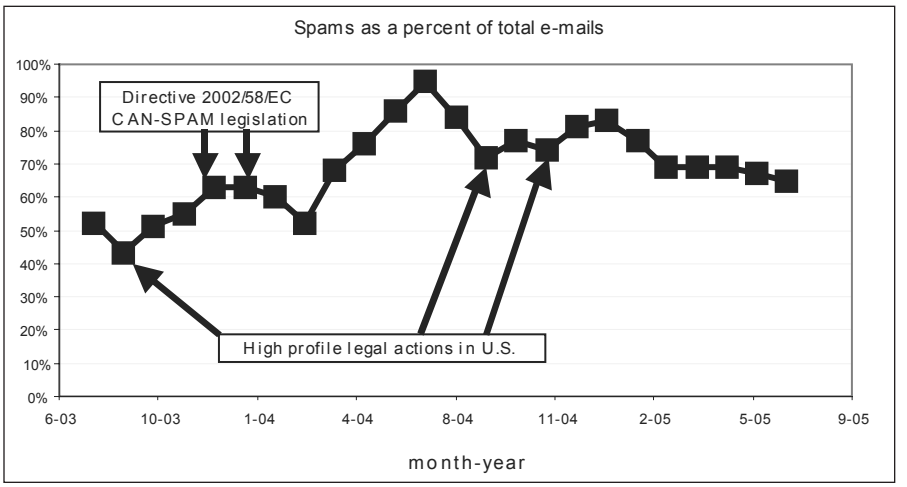
Year	Worldwide Economic Impact (US$)
2003	$13.5 Billion
2002	11.1 Billion
2001	13.2 Billion
2000	17.1 Billion
1999	12.1 Billion
1998	6.1 Billion
1997	3.3 Billion
1996	1.8 Billion
1995	500 Million

Table 4. Financial impact of major virus attacks since 1999 (Source: http://www.computereconomics.com)

Year	Code Name	Worldwide Financial Impact ($US)
2004	MyDoom	$4.0 Billion
2003	SoBig.F	2.5 Billion
2003	Slammer	1.5 Billion
2003	Blaster	750 Million
2003	Nachi	500 Million
2002	Klez	750 Million
2002	BugBear	500 Million
2002	Badtrans	400 Million
2001	CodeRed	2.75 Billion
2001	Nimda	1.5 Billion
2001	SirCam	1.25 Billion
2000	ILOVEU	8.75 Billion
1999	Melissa	1.5 Billion
1999	Explorer	1.1 Billion

However, there are limits to what can be achieved through the enactment of new criminal and civil laws to deal with illicit electronic activities, just as there are limits to what the law can achieve more generally. Civil litigation is an expensive and uncertain process. Judgments can be difficult to enforce against defendants that are determined to avoid payment. Criminal laws have not eliminated crime. The global nature of the Internet means that laws have to be coordinated and enforced across international borders, introducing further complications. As a result, managing electronic risk requires a blend of risk reduction and legal strategies.

Figure 1. Spam has become a huge segment of e-mails



A Catalog of Risks and Legal Problems

The most common electronic risks are the following: (1) business interruptions caused by hackers, cybertheives, viruses, and internal saboteurs; (2) employer liability stemming from the inappropriate employee use of e-mail and Internet; (3) claims that products and services advertised on the Web fail to deliver; (4) Web-related copyright and trademark lawsuits; (5) patent infringement costs; (6) fraud-extortion hybrid.

General Legal Issues

Given the international scope cyberspace, several general legal issues arise. The first is how to address conflicts between the laws of different jurisdictions. Whose law governs when the parties involved live in different countries and the transaction occurs in cyberspace? Many Web sites now use online contracts that specifically provide whose law will govern the transaction. These online contracts generally require the user to click their agreement with the terms of the contract before they are allowed to proceed with the transaction.

A related issue is choice of forum. Where do you sue for breach of contract? Many online contracts also provide the answer to this question. However, where there is no contract involved, such as in cases of fraud or negligence, the issues of conflict of laws and choice of forum may not have clear answers. Moreover, the choice of forum that is of the most benefit to the party who is suing for damages will be the jurisdiction in which the assets are located that will serve to satisfy any award for damages. Alternatively, the plaintiff may prefer to sue in its own jurisdiction due to convenience or familiarity with the system.

If a plaintiff chooses to sue in a particular jurisdiction, that does not resolve the matter. In each jurisdiction, courts apply their own rules to determine whether to exercise jurisdiction over the defendant in a given case. For example, many U.S. courts base the decision to accept jurisdiction in Internet transactions on the nature and quality of the commercial activity. If a foreign defendant enters into contracts with residents in the jurisdiction that involve knowing and repeated transmission of computer files over the Internet, the court will accept jurisdiction. On the other hand, if the defendant merely operates a passive Web site that posts information that is accessible

to users in other jurisdictions, the court will not exercise jurisdiction (Gasparini, 2001).

One crucial question is, who do you sue? In cases involving employees, it is generally wise to sue both the individual and the employer. In determining who to sue, several questions must be considered. Who has liability? Who has assets that can be seized to satisfy a judgment awarding damages? Where are the assets? What is the procedure to seize the assets in the jurisdiction in which they are located? Are the assets accessible? For example, are they held in the name of the responsible person and in a jurisdiction where the judgment can be enforced? In some jurisdictions, enforcing judgments may be problematic. For example, in Mexico, bank secrecy laws may prevent a determination of what assets are available to satisfy a judgment. In addition, enforcing the judgments of courts from one country in a second country can be problematic where the second country has no procedure for recognizing the awards of foreign courts.

Another important consideration is litigation risk. Litigation is costly and the outcome is uncertain. Even if the plaintiff secures judgment in his favor, enforcement may not be possible. If the party claiming damages is not able to collect from the guilty party, the cost of litigation is wasted. This leads to another important question. Is the guilty party insured? Does the insurance contract provide coverage for actions that generated legal liability? Should it?

BUSINESS INTERRUPTIONS

Any kind of business interruption is costly. It can increase cost of doing business or reduce revenue or both. It does not matter if it stems from strikes, fire, power failure, hackers or saboteurs. Electronic risk is increasingly becoming a bigger threat to business.

For example, a hacker overwhelmed several large Web sites through multiple distributed denial-of-service (DDOS) attacks. The culprit hijacked various computers throughout the world to bombard target servers with seemingly legitimate requests for data. It is estimated that the DDOS attacks, which interrupted the sites' ability to efficiently conduct their business, caused over $1.2 billion in lost business income. (http://www.insurenewmedia.com/html/claimsexample.htm)

This raises several legal issues. The denial of service that occurs when the server fails could expose the business to claims for damages for breach of contract from clients. In the contract, the server agrees to provide the service. If the interruption of service causes financial loss, for example, due to lost business, the administrator of the server may be liable for the loss. Liability will depend on the terms of each contract. For example, if a *force majeure* clause excuses the server from performing the contract in the event of power outages or hacker attacks, there will be no liability.

The denial of service could also give rise to a claim for damages based on the negligence of the server administrator. Where the server can be protected against hacker attacks by readily available technology, the failure of administrator to employ the technology to protect client access to the service would be negligent.

Another issue is whether the server may sue the hacker for damages. However, this may be a moot point if the hacker cannot be located, lives in a jurisdiction where the law does not allow for such a legal claim to be filed, or has no assets with which to satisfy the claim for damages (for example, teenage hackers with poor parents).

INAPPROPRIATE USE OF E-MAIL AND INTERNET

Inappropriate use of e-mail and Internet can expose employers to claims for damages in three principal areas of law—human rights law, privacy legislation, and civil liability for damages caused

by employees to fellow employees or third parties under negligence and libel laws.

In addition to the foregoing liability risks, e-mail communications are a rich source of evidence in any kind of legal dispute, which means that employees need to be careful about what they communicate electronically. Poorly managed written communications in e-mails and letters can come back to haunt any business that later finds itself enmeshed in litigation, accused of corporate fraud, or audited for SEC compliance. It is technically possible to recover e-mail messages that have been "deleted" in e-mail programs, making it difficult to destroy this type of evidence. As a result, these messages may be uncovered during a civil litigation procedure known as pretrial discovery in common-law jurisdictions such as Canada and the United States. This data needs to be managed well, both in terms of limiting its creation in the first place and in terms of reducing the cost of its retrieval should it need to be produced in pretrial discovery. (Just imagine the cost of teams of lawyers sorting through millions of e-mails.)

Many jurisdictions give employees the right to sue for sexual harassment under human rights legislation. A common inappropriate use of e-mail consists of sexual harassment of one employee by another. For example, a manager and his employer could be sued for communicating sexual messages via e-mail to a subordinate. The same act can create a cause of action for a civil suit against both the manager and the employer who allowed the act to take place. In litigation, reliable evidence that the harassment really took place becomes a central issue. When the means of communication is e-mail, that evidence is more readily available, increasing the risk of an award of damages against the employer.

Electronic communication raises the risks of violating general privacy legislation and professional rules regarding privileged information. One of largest health insurers in the United States inadvertently sent e-mail messages to 19 members containing confidential medical and personal information of 858 other members. Although the company immediately took steps to correct the problem, the company was exposed to lawsuits alleging invasion of privacy. Similarly, lawyers must take care not to violate solicitor-client privilege, which can expose them to both disciplinary proceedings in the profession and claims for damages from the client (Rest, 1998).

Internet telecommuting raises the risk that an employer's internal network will be exposed to "backdoor attacks" that exploit the telecommuter's connection and threaten confidential information belonging to a client or third party. In such cases, employer liability will probably depend on whether the employer provided adequate protection from such an attack (Maier, 2001).

Employee use of company e-mail to promote personal business is another source of legal problems. Where the actions of the employee can be considered part of the normal course of their employment duties, the employer may be held liable for the actions of the employee. For example, the employer may be liable for allowing its system to be used for the communication of the slanderous message. In the United States, however, the Communications Decency Act of 1996 has made Internet providers immune from liability for publishing a defamatory statement made by another party and for refusing to remove the statement from its service (King, 2003).

The employer may be held liable for failing to properly supervise employee use of e-mail and Internet. For example, an employee who uses e-mail to sexually harass a fellow employee can expose a company to lawsuits. Using the company's e-mail and Internet system to further criminal acts can also expose the company to liability. In such cases, traditional law regarding employer liability extends to e-risk cases.

Under the common law doctrine of *respondeat superior*, the employer is responsible for employee acts that are within the scope of employment or further the employer's interests. However, the

employer cannot be held liable if the personal motives of the employee are unrelated to the employer's business. (Nowak, 1999) For example, in Haybeck vs. Prodigy Services Co., Prodigy Services was not held liable for the actions of a computer technical advisor when he used the company computer to enter Internet chat rooms and to lure his victim with offers of free time on Prodigy. The employee was HIV-positive and intentionally had unprotected sex without disclosing his infection. Where an employee's improper use of e-mail or Internet falls outside the scope of employment, the employer cannot be held liable under this doctrine.

However, the employer may still be found liable for negligently retaining or supervising an employee. Under the doctrine of negligent retention, an employer may be liable for hiring an unfit person in circumstances that involve an unreasonable risk of harm to others. The employer will be held liable for the acts of an employee where the employer knew or should have known about the employee's conduct or propensity to engage in such conduct. Moreover, the employer has a duty to set rules in the workplace and to properly supervise employees. (Nowak, 1999) Thus, there is a risk of liability if the employer has knowledge of facts that should lead the employer to investigate an employee or to implement preventive rules for all employees.

The key issue is whether the employer could have reasonably foreseen the actions of the employee. For example, in the Prodigy case, the court held that the employer was not liable for negligent retention because the plaintiff could not show that Prodigy had any knowledge of his activities. Nor was there an allegation that technical advisors commonly have sex with customers without revealing that they carry communicable diseases. However, in Moses vs. Diocese of Colorado, a church parishioner in Colorado successfully sued the Episcopal diocese and bishop for injuries she suffered having sex with a priest from whom she sought counseling. Sexual relationships between priests and parishioners had arisen seven times before and the diocese had been notified that greater supervision of the priests might be necessary. The court found the diocese negligent for not providing more supervision when it knew that such relationships were becoming more common.

Similarly, employers may be held liable for negligent supervision of employee use of e-mail and Internet if they know that their employees visit pornographic Internet sites and use e-mail for personal communications. In such circumstances, they have a duty to provide rules of conduct for employees and to monitor compliance. If they administer their own networks, they should monitor employee use of the system where incriminating communications may be stored. It would be difficult to argue that they are unaware of employee activities when contradictory evidence is stored on the company system. Employers should use software that blocks access to pornographic Internet sites and that screens e-mails for key words. However, they should also advise employees that their computer use is being monitored, to avoid liability for invasion of employee privacy.

A company's monitoring practices may be justified by the potential liabilities created by employees' misuse of e-mail and the Internet. However, the company's potential liability for invasion of employee privacy must also be considered. While employees in the United States have little privacy protection in this area, European employers must take reasonable precautions to protect their employees' privacy when they monitor their e-mail or Internet usage. (Rustad & Paulsson, 2005). Even in the United States, however, employers should take care not to violate labor laws by unduly restricting their employees' communications regarding labor rights (O'Brien, 2002).

Companies can reduce or eliminate the risk of liability for employees' use of electronic communication by implementing an effective Internet policy. Such a policy should (1) warn employees that their communications may be monitored; (2) require employees to sign consent forms for

monitoring; (3) limit employee Internet access to work-related activities; (4) establish clear rules against conducting personal business on the company system; (5) define and prohibit communications that may be considered harassment of fellow employees and third parties or violate human rights laws; (6) forbid employees using another employee's system; (7) implement a policy on the length of time documents are retained on a backup system; and (8) ensure all employees understand and will follow the policy. (Nowak, 1999) To limit exposure to e-risk, insurers should insist that clients implement an effective Internet policy as a condition of coverage.

Sloan (2004) offers a series of practical suggestions for avoiding litigation problems. His advice includes the following recommendations: (1) Instead of using e-mails, it is preferable to use telephones when possible. (2) E-mails should not be sent immediately. Once sent, e-mails cannot be called back. If a cooling period is implemented, they can be recalled. (3) The distribution of e-mails should be limited. The default e-mail option should not include the possibility of sending it to a large group within a company all at once. (4) Within a company, sarcasm and criticism can do a lot of damage to the company's health. They should be avoided. (5) Swearing is a bad idea in an e-mail. This should be avoided at all cost.

FAILURE OF PRODUCT

Failure of a product to deliver can come from many different sources. For example, an antivirus software may fail to protect the customer from a particular virus leading to loss of mission-critical data for the company. Recently, a number of Web site development companies have been sued for being negligent with their design, which allowed hackers to enter and use computer portals for unauthorized use.

False claims regarding the characteristics of products and services can give rise to three types of legal actions. If it is a case of fraud, criminal laws would govern. Criminal legal procedures differ from civil law suits in two important respects. The cost of filing a criminal complaint is negligible because the investigating police and the prosecutor are paid by the state. This provides a low financial threshold for the unhappy customer. However, defending a criminal charge is just as costly as defending a civil action for the business person who commits the fraud. However, a criminal case generally results in no damages award. Instead, the guilty party may be subject to fines and/or imprisonment. The customer thus has a low financial threshold for filing charges, but is likely to receive no financial reward at the conclusion of the proceedings, except in cases where courts order the defendant to pay restitution.

In many jurisdictions, consumer protection legislation gives customers the right to return a product for a refund where the product is not suitable for the purpose for which it is intended. As long as the business provides the refund, the cost to the business is relatively low because its liability ends with the refund. Should the business refuse to refund the purchase price, the customer may sue and be entitled to legal costs as well. However, where the value of the transaction is low, the cost of suing will exceed the amount owing, making it impractical to pursue.

In common law jurisdictions (such as Australia, Canada, England, and the United States), false claims regarding a product or service may give rise to a civil action for negligent misrepresentation. In a case of negligent misrepresentation, the customer could claim compensation for damages caused by the customer's reliance on the company's representation of what the product or service would do.

Traditional principles of agency may expose reputable companies to liability where they sponsor the Web sites of smaller firms. If the company creates the appearance of an agency relationship, and a consumer reasonably believes the companies are related, the consumer can sue the sponsor for

the harm caused by the lack of care or skill of the apparent agent. This is so even where no formal agency relationship exists (Furnari, 1999).

FRAUD, EXTORTION, AND OTHER CYBERCRIMES

The Internet facilitates a wide range of international crimes, including forgery and counterfeiting, bank robbery, transmission of threats, fraud, extortion, copyright infringement, theft of trade secrets, transmission of child pornography, interception of communications, transmission of harassing communications and, more recently, cyberterrorism. However, the division of the world into separate legal jurisdictions complicates the investigation and prosecution of transnational cybercrimes (Goldstone & Shave, 1999).

There are numerous examples. In one case, eight banking Web sites in the United States, Canada, Great Britain, and Thailand were attacked, resulting in 23,000 stolen credit card numbers. The hackers proceeded to publish 6,500 of the cards online, causing third-party damages in excess of $3,000,000 (http://www.aignetadvantage.com/bp/servlet/unprotected/claims.examples). In another case, a computer hacker theft ring in Russia broke into a Citibank electronic money transfer system and tried to steal more than $10 million by making wire transfers to accounts in Finland, Russia, Germany, The Netherlands, and the United States. Citibank recovered all but $400,000 of these transfers. The leader of the theft ring was arrested in London, extradited to the United States 2 years later, sentenced to 3 years in jail, and ordered to pay $240,000 in restitution to Citibank. In yet another case, an Argentine hacker broke into several military, university, and private computer systems in the United States containing highly sensitive information. U.S. authorities tracked him to Argentina and Argentina investigated his intrusions into the Argentine telecommunications system. However, Argentine law did not cover his attacks on computers in the United States, so only the United States could prosecute him for those crimes. However, there was no extradition treaty between Argentina and the United States. The U.S. persuaded him to come to the United States and to plead guilty, for which he received a fine of $5,000 and 3-years probation (Goldstone & Shave, 1999).

In these types of scenarios, the hackers could be subject to criminal prosecution in the victim's country but not in the perpetrator's home country. Even if subject to criminal prosecution in both countries, extradition may not be possible. Moreover, criminal proceedings would probably not fully compensate the banks for their losses or that of their customers. Indeed, the customers might be able to file claims against the banks for negligence if they failed to use the latest technology to protect their clients' information from the hackers.

A further complication arises when there are conflicts between the laws of different countries. For example, hate speech (promoting hatred against visible minorities) is illegal in countries such as Canada, but protected by the constitution in the United States. A court may order the production of banking records in one country that are protected by bank secrecy laws in another. For example, in United States vs. Bank of Nova Scotia, the Canadian Bank of Nova Scotia was held in contempt for failing to comply with an order that required the bank to violate a Bahamian bank secrecy rule.

The jurisdictional limits of the authorities in each country also complicate investigations. For example, a search warrant may be issued in one country or state to search computer data at a corporation inside the jurisdiction, but the information may actually be stored on a file server in a foreign country, raising issues regarding the legality of the search. International investigations are further complicated by the availability of

experts in foreign countries, their willingness to cooperate, language barriers, and time differences (Goldstone & Shave, 1999).

Another cybercrime that is currently theoretical is cyberterrorism. While there have been no cases to date, there are likely to be in the future. A bill passed by the New York Senate defines the crime of cyberterrorism as any computer crime or denial of service attack with an intent to ... influence the policy of a unit of government by intimidation or coercion, or affect the conduct of a unit of government (Iqbal, 2004).

WEB-RELATED INTELLECTUAL PROPERTY RIGHTS INFRINGEMENT

Intellectual property infringements are a significant liability risk for Internet business and may lead to expensive litigation. For example, computer bulletin board companies have been sued for copyright infringement (in Religious Technology Center vS. Netcom Online Communication Services, Inc.) and for copyright infringement, trademark infringement, and unfair competition with respect to video games (in Sega Enterprises Ltd. vs. Maphia). (Richmond, 2002) In another case, an online insurance brokerage created a hyperlink that seemingly transferred its clients to additional pages on the site itself. It was later discovered that the brokerage "deep-linked" its users to the Web pages of various insurance companies, creating a seamless navigational experience. The insurance companies sued the online brokerage for copyright and trademark infringement (http://www.insurenewmedia.com/html/claimsexample.htm). With litigation of intellectual property claims against e-commerce ventures on the rise, the risk is increasing for insurance companies as well (General & Cologne Re, 1999).

Patent infringement claims are quite common. In the past, Microsoft had faced a whole slew of them (including the well-publicized ones from Xerox about the use of mouse as a computer interface). Computer software always builds on past programs. Therefore, the line between what is legal and what is not is not very clear (see, for example, http://www.borland.com/about/press/2001/webgainsuit.html for a recent lawsuit by Borland against WebGain).

Cybersquatters have led to the further development of trademark law. In the early days to the Web, cybersquatters registered Web sites using the names of well-known companies and celebrities. Many made substantial amounts of money later selling the name back to the company or individual. However, their joy ride ended with cases such as Madonna's, who successfully sued to claim the Web site name without paying the cybersquatter.

Intellectual property law protects legal rights such as those related to copyrights, patents, and trademarks. Intellectual property law has been globalized by several international agreements. Countries that are members of the North American Free Trade Agreement (NAFTA) (Canada, the U.S., and Mexico) and the World Trade Organization (WTO) (148 countries) are required to have laws providing both civil and criminal procedures for the enforcement of copyright and trademarks. In this regard, the requirements of NAFTA Chapter 17 and the WTO Agreement on Trade-Related Intellectual Property Rights (TRIPS) are virtually the same.

TRIPS requires members to make civil judicial procedures available to right holders, including minimum standards for legal procedures, evidence, injunctions, damages, and trial costs (TRIPS Articles 42-49). Rights holders may thus seek court injunctions to stop the illegal activity and have the perpetrator ordered to pay the costs of the legal action. The owners of intellectual property may sue producers and vendors of pirated goods for damages. While this is important, in many cases it is not a practical option for companies to pursue. Civil litigation is a costly and lengthy process, and seeking payment

Table 5. Pirated software in use and the losses due to piracy in 2003 and 2004 (Source: Second Annual BSA and IDC Global Software Piracy Study, 2005)

	% software pirated	% software pirated	Loss due to piracy in millions of $US	Loss due to piracy in millions of $US
Country	2004	2003	2004	2003
Australia	32%	31%	409	341
China	90%	92%	3,565	3,823
Hong Kong	52%	52%	116	102
India	74%	73%	519	367
Indonesia	87%	88%	183	158
Japan	28%	29%	1,787	1,633
Malaysia	61%	63%	134	129
New Zealand	23%	23%	25	21
Pakistan	82%	83%	26	16
Philippines	71%	72%	69	55
Singapore	42%	43%	96	90
South Korea	46%	48%	506	462
Taiwan	43%	43%	161	139
Thailand	79%	80%	183	141
Vietnam	92%	92%	55	41
Austria	25%	27%	128	109
Belgium	29%	29%	309	240
Cyprus	53%	55%	9	8
Czech Republic	41%	40%	132	106
Denmark	27%	26%	226	165
Estonia	55%	54%	17	14
Finland	29%	31%	177	148
France	45%	45%	2,928	2,311
Germany	29%	30%	2,286	1,899
Greece	62%	63%	106	87
Hungary	44%	42%	126	96
Ireland	38%	41%	89	71
Italy	50%	49%	1,500	1,127
Latvia	58%	57%	19	16
Lithuania	58%	58%	21	17
Malta	47%	46%	3	2
Netherlands	30%	33%	628	577
Poland	59%	58%	379	301
Portugal	40%	41%	82	66
Slovakia	48%	50%	48	40
Slovenia	51%	52%	37	32

continued on next page

Table 5. continued

Spain	43%	44%	634	512
Sweden	26%	27%	304	241
United Kingdom	27%	29%	1,963	1,601
Bulgaria	71%	71%	33	26
Croatia	58%	59%	50	45
Norway	31%	32%	184	155
Romania	74%	73%	62	49
Russia	87%	87%	1,362	1,104
Switzerland	28%	31%	309	293
Ukraine	91%	91%	107	92
Argentina	75%	71%	108	69
Bolivia	80%	78%	9	11
Brazil	64%	61%	659	519
Chile	64%	63%	87	68
Colombia	55%	53%	81	61
Costa Rica	67%	68%	16	17
Dominican Republic	77%	76%	4	5
Ecuador	70%	68%	13	11
El Salvador	80%	79%	5	4
Guatemala	78%	77%	10	9
Honduras	75%	73%	3	3
Mexico	65%	63%	407	369
Nicaragua	80%	79%	1	1
Panama	70%	69%	4	4
Paraguay	83%	83%	11	9
Peru	73%	68%	39	31
Uruguay	71%	67%	12	10
Venezuela	79%	72%	71	55
Algeria	83%	84%	67	59
Bahrain	62%	64%	19	18
Egypt	65%	69%	50	56
Israel	33%	35%	66	69
Jordan	64%	65%	16	15
Kenya	83%	80%	16	12
Kuwait	68%	68%	48	41
Lebanon	75%	74%	26	22
Mauritus	60%	61%	4	4
Morocco	72%	73%	65	57
Nigeria	84%	84%	54	47
Oman	64%	65%	13	11

continued on next page

Table 5. continued

Qatar	62%	63%	16	13
Reunion	40%	39%	1	1
Saudi Arabia	52%	54%	125	120
South Africa	37%	36%	196	147
Tunisia	84%	82%	38	29
Turkey	66%	66%	182	127
UAE	34%	34%	34	29
Zimbabwe	90%	87%	9	6
Canada	36%	35%	889	736
Puerto Rico	46%	46%	15	11
United States	21%	22%	6,645	6,496

of any damages that might be awarded can be problematic. Nevertheless, the global expansion of intellectual property law remedies, together with the global nature of the Internet, is sure to increase intellectual property litigation around the globe.

TRIPS also requires members to provide criminal procedures and penalties in cases of intentional trademark counterfeiting or copyright piracy on a commercial scale. Penalties must include imprisonment or fines sufficient to provide a deterrent, consistent with the level of penalties applied for crimes of a corresponding gravity. Where appropriate, remedies must also include the seizure, forfeiture, and destruction of the infringing goods (TRIPS Article 61).

As tough as this may sound, such criminal laws do not have a great impact on the enforcement of intellectual property laws in many developing countries. While authorities may occasionally conduct well-publicized raids on highly visible commercial operations, corruption and the lack of adequate human and financial resources means the vast majority of infractions still go unpunished. These practical and legal limitations inherent in intellectual property protection mean that producers of easily copied intellectual property, such as software, are likely to continue to experience worldwide problems with piracy, as the following table shows (Table 5). The amount of money at stake, together with the globalization of intellectual property laws, means that owners of intellectual property are likely to devote more of their own resources to the enforcement of their property rights in the coming years.

Insurance

In August 2000, St Paul insurance company commissioned a survey of 1,500 risk managers in the United States and Europe, along with 150 insurance agents and brokers. Only 25% of all U.S. companies and 30% of European companies had set up formal structures (such as a risk management committee) to identify and monitor technology risks.

Online attack insurance costs between $10,000 and $20,000 per million-dollar coverage. Main coverage takes the following forms: protection against third-party liability claims from the disclosure of confidential information when a hacker strikes or denial of service when a computer virus attacks. Another common coverage is electronic publishing liability, which can offer protection

from third-party lawsuits for defamation, libel, slander, and other claims stemming from information posted on the company Web site.

While many of the legal sources of liability for online activity are not new (such as intellectual property infringements, defamation, and invasion of privacy), the accessibility of the Internet has increased the rapidity and scale of these actions and, thus, the potential liability. As a result, some believe that e-commerce will emerge as the single biggest insurance risk of the 21st century, for three reasons. First, the number of suits involving Internet-related claims will be exponentially greater than in pre-Internet days. Second, the complexity of international, multi-jurisdictional and technical disputes will increase the legal costs associated with these claims. Third, the activities giving rise to Internet-based claims will present new arguments for both insureds and insurers about whether they the liability is covered by the policy (Jerry & Mekel, 2002). For example, traditional first party insurance for physical events that damage tangible property may not help an Internet business whose most valuable property exists in cyberspace with no physical form (Beh, 2002). Even if a company has an insurance policy that covers its activities on the World Wide Web, there is a significant risk that it won't be covered outside the United States or Canada (Crane, 2001).

CONCLUSION

Like the more traditional marketplace, doing business on the Internet carries with it many opportunities along with many risks. This chapter has focused on a series of risks of legal liability arising from e-mail and Internet activities that are a common part of many e-businesses. Some of the laws governing these electronic activities are new and especially designed for the electronic age, while others are more traditional laws whose application to electronic activities is the novelty.

E-business not only exposes companies to new types of liability risk, but also increases the potential number of claims and the complexity of dealing with those claims. The international nature of the Internet, together with a lack of uniformity of laws governing the same activities in different countries, means that companies need to proceed with caution. That means managing risks in an intelligent fashion and seeking adequate insurance coverage. The first step is to familiarize themselves with electronic risks and then to set up management systems to minimize potential problems and liabilities.

ACKNOWLEDGMENT

We thank the Instituto Tecnológico Autónomo de México and the Asociación Mexicana de Cultura AC for their generous support of our research.

REFERENCES

Beh, H. G. (2002). Physical losses in cyberspace. *Connecticut Insurance Law Journal, 9*(2), 1-88.

Crane, M. (2001). International liability in cyberspace. *Duke Law and Technological Review, 23*(1), 455-465.

Furnari, N. R. (1999). Are traditional agency principles effective for Internet transactions, given the lack of personal interaction? *Albany Law Review, 63*(3), 544-567.

Gasparini, L. U. (2001). The Internet and personal jurisdiction: Traditional jurisprudence for the twenty-first century under the New York CPLR. *Albany Law Journal of Science & Technology, 12*(1), 191-244.

General, & Cologne Re. (1999). *Global casualty facultative loss & litigation report: A selection of Internet losses and litigation, 3*, 12-17.

Goldstone, D. & Shave, B. (1999). International dimensions of crimes in cyberspace. *Fordham International Law Journal, 22*(6), 1924-1945.

Iqbal, M. (2004). Defining cyberterrorism. *Marshall Journal of Computer & Information Law, 22*(1) 397-432.

Jerry, R. H. II, & Mekel, M. L. (2002). Cybercoverage for cyber-risks: An Overview of insurers' responses to the perils of e-commerce. *Connecticut Insurance Law Journal, 9*(3), 11-44.

King, R. W. (2003). Online defamation: Bringing the Communications Decency Act of 1996 in line with sound public policy. *Duke Law and Technology Review, 24*(3), 34-67.

Maier, M. J. (2001). Backdoor liability from Internet telecommuters. *Computer Law Review & Technology Journal, 6*(1), 27-41.

Marron, M. (2002). Discoverability of deleted e-mail: Time for a closer examination. *Seattle University Law Review, 25*(4), 895-922.

Nowak, J. S. (1999). Employer liability for employee online criminal acts. *Federal Communications Law Journal, 51*(3) 467-488.

O'Brien, C. N. (2002). The impact of employer e-mail policies on employee rights to engage in concerted. *Dickinson Law Review, 103*(5), 201-277.

Pederson, M., & Meyers, J. H. (2005). Something about technology: Electronic discovery considerations and methodology. *Maine Bar Journal, 12*(2), 23-56.

Rest, C. L. (1998). Electronic mail and confidential client/attorney communications: Risk management. *Case Western Reserve Law Journal, 48*(2), 309-378.

Richmond, D. R. (2002). A practical look at e-commerce and liability insurance. *Connecticut Insurance Law Journal, 8*(1), 87-104.

Rustad, M. L., & Paulsson, S. R. (2005). Monitoring employee e-mail and Internet usage: Avoiding the omniscient electronic sweatshop: Insights from Europe. *University of Pennsylvania Journal of Labor and Employment, 7*(4), 829-922.

Sloan, B. (2004, July). Avoiding litigation pitfalls: Practical tips for internal e-mail. *Risk Management Magazine*, 38-42.

APPENDIX: TERMINOLOGIES

Firewall: A firewall is a barrier that enforces a boundary between two or more computer networks. It is similar to the function of firewalls in building construction. A firewall controls traffic between different zones of trust. Two extreme zones of trust include the Internet (a zone with no trust) and an internal network (a zone with high trust). Setting up firewalls requires understanding of network protocols and of computer security. Small mistakes can render a firewall worthless as a security tool.

Hackers: In computer security, a hacker is a person able to exploit a system or gain unauthorized access through skill and tactics. This usually refers to a black-hat hacker. Two types of distinguished hackers exist. A Guru is one with a very broad degree of expertise, a Wizard is an expert in a very narrow field.

Malware: Malware is a software program that runs automatically against the interests of the person running it. Malware is normally classified based on how it is executed, how it spreads, and what it does.

Phishing: Phishing (also known as carding and spoofing) is an attempt to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an apparently official electronic communication, such as an e-mail. The term phishing alludes to to "fishing" for users' financial information and passwords.

Spam: Spam refers to unsolicited messages in bulk. It can refer to any commercially oriented, unsolicited bulk mailing perceived as being excessive and undesired. Most come in e-mail as a form of commercial advertising.

Spoofing: See *phishing.*

Spyware: Spyware is a malicious software intended to intercept or take control of a computer's operation without the user's knowledge or consent. It typically subverts the computer's operation for the benefit of a third party.

Virus: A virus is a self-replicating program that spreads by inserting copies of itself into other executable code or documents. A computer virus behaves in a way similar to a biological virus. The insertion of the virus into a program is called an infection, and the infected file (or executable code that is not part of a file) is called a host. A virus is a malware.

Worm: A computer worm is a self-replicating computer program. A virus needs to attach itself to, and becomes part of, another executable program. A worm is self-contained. It does not need to be part of another program to propagate itself.

This work was previously published in E-Business Process Management: Technologies and Solutions, edited by J. Sounderpandian and T. Sinha, pp. 292-311, copyright 2007 by IGI Publishing, formerly known as Idea Group Publishing (an imprint of IGI Global).