LIABILITY FOR BREACH OF E-COMMERCE SECURITY STANDARDS

by Katie Matison

I. INTRODUCTION

The exponential growth of internet-based commercial transactions and the electronic storage of sensitive data have cultivated a fertile environment for disclosing private data, transmission of destructive viruses and theft of consumer information. Last year, internet advertising exceeded $5.3 billion. In 1999, computer hackers cost United States corporations $266 million in damages and business losses. According to a report by the Computer Emergency Response Team at the Carnegie Mellon Institute in Pittsburgh, Pennsylvania, 8,300 incidents of computer hackers were reported in 1999,[1] which tripled the reported cases in 1998. As a result of the significant commercial losses and third party liability for the disclosure of sensitive data, online security has become a preeminent concern of businesses and underwriters insuring businesses conducting online transactions.[2]

II. LIABILITY FOR SECURITY BREACHES

Vulnerable security systems which allow the misuse, exposure and exploitation of private or sensitive data create tortious third-party liability in the United States. Moreover, commercial

---

[1] McDonald, Tim, ECommerce Times, *Top 10 List Reveals Internet Security Flaws*, June 2, 2000. www.Ecommerce.Times.com. The article reports that the Systems Administration, Networking and Security Institute published a top 10 list of the most popular methods utilized by hackers to penetrate network servers and computer systems. Ineffective and vulnerable security systems have been cited as the principle window of opportunity for a computer hacker.

[2] E-Commerce Law Weekly, characterized online security as follows:

> According to Deidre Mulligan, at the Center for Democracy and Technology, the online industry is in the early stages of building an identification and authentication infrastructure. This infrastructure is basically a network system for identifying who a person is online and whether they are authorized to do something -- engage in a commercial transaction, alter their private medical data or otherwise engage in communications that need identification, authentication and security.

establishments may also suffer significant financial losses as a result of business interruption and the irretrievable destruction of important data caused by a computer hacker. Also, the unauthorized downloading of trade secrets or mere possession of certain unauthorized information subjects businesses to criminal liability. These issues are separately considered below.

A. Liability to Third-Parties.

Recently, the incidents of exposure of private customer data have increased in frequency. In February 2001, a security breach on the website of Columbia House, a major music company, exposed thousands of its customers' names, addresses and portions of their credit card numbers. The breach also exposed company coupon codes, log files, names and passwords to Columbia's main database. Similarly, in January 2001, Travelocity reported a security breach exposing the personal data of thousands of its customers purchasing on-line travel services. In December, 2000, over 3.7 million customer accounts were potentially exposed by a hacker who penetrated the computer system of Egghead.com. Additionally, CreditCards.com, IKEA and Amazon.com suffered community breaches by hackers.[3]

In July 2000, Nike, Inc.'s website was penetrated by a hacker and Nike information was diverted to an anti-Nike activist site in Australia. Scottish ISP First Net On-Line redirected e-mail traffic back to Nike and later asserted a claim for negligent internet security against the shoe manufacturer.[4] The Nike/Scottish ISP dispute has been cited as the potential watershed of an avalanche of negligent internet security claims over the next few years.[5]

E-commerce Law Weekly, "*Panel Says Online Security Is More Than Just Encryption Problem,*" April 20, 2000.
[3] Olsen, Stephanie, CNET News.com "*Columbia House Breach Exposes Customer Info*," February 2, 2001.
[4] Id.
[5] Id.

Several other examples of security breaches resulting in potential third-party liability are as follows:[6]

- According to the chairman of the Federal Trade Commission, sexual predators often surf bulletin boards seeking information regarding minors. The exposure of information to a sexual predator as a result of a vulnerable security system could potentially create third-party liability of the respective companies for negligence, invasion of privacy, negligent infliction of emotional distress, and in venues other than Washington punitive damages.

- An insecure system which exposes customer information including credit cards, Social Security numbers, banking information, credit history data and personal medical information could create liability for negligence, invasion of privacy, negligent infliction of emotional distress, the tort of outrage, and in some instances, property damage.

- The destruction of private confidential data which becomes irretrievably lost as a result of either a computer hacker or a computer virus may create third-party liability to a third party for negligence, invasion of privacy or property damage. If in fact the commercial entity has made representations as to its superior abilities for the safekeeping of private data, it could be held to a standard of strict liability or *great care* as well as liability for the breach of contract.

- A corporate entity may be deemed negligent for the transmission of a destructive virus to a third party as a result of an inadequate security system. To date, claims have been asserted against companies whose actions caused the transmission of viruses. [7]

- The publication Daily News recently reported suits by injured parties against companies whose computer systems were hijacked for denial of service attacks.[8]

These examples illustrate that it is mandatory for a corporate entity conducting commercial transactions over the internet to maintain *reasonable security standards which*

---

[6] Although various claims have been made, there are not any reported decisions on this issue and most cases will be a matter of first impression. One court noted:

> We observed that the lightning speed development of the Internet poses challenges for the common law adjudicative process -- a process which, ideally while grounded in the past, governs the present and offers direction for the future based on understandings of current circumstances.

Name. Space v. Network Solutions, Inc., 202 F.3d 573 (2nd Cir. 2000).

[7] Will Garside, Daily News, "*Hackers Dupes Could Face Legal Threat*," 14 February 2001.

[8] Id.

comply with state of the art technology.[9] The failure to maintain reasonable security precautions will likely be deemed a breach of the duty of due care and resulting third-party liability. Third-party liability potentially may be asserted against a company for its failure to maintain reasonable security standards under theories of negligence, invasion of privacy, negligent infliction of emotional distress, outrage, property damage and in some instances breach of contract. Moreover, in certain circumstances, a company may have liability for great care and in states other than Washington could be subjected to punitive damages.

B. First-Party Business Losses.

Inadequate security systems increase the potential for business interruption losses and the costly destruction of business records and sensitive data. These concerns also extend to wireless viruses. For example, in September 2000, many wireless users were affected by the Liberty Crack virus, a palm pilot Trojan horse disguised as a GameBoy emulator that deleted files. As a result of the threat to wireless security, certain experts recommend procedures to obviate the potential for wireless security fraud. These include: (i) changing security codes on the network and devoiding default codes open to any third party; (ii) isolating the access points and path through which wireless users gain access to the network; (iii) providing central IT support to departmental wireless networks; (iv) implementing media access control address tracking to isolate the identity of individuals traveling on the network and to allow disabling stolen wireless devices; and (v) monitoring access logs.[10]

C. Criminal Liability.

[9] The health care financing administration regulations promulgated pursuant to the Health Insurance Portability and Accountability Act of 1996 require that U.S. health care providers must meet stringent security and privacy regulations. This Act protects patient data from unauthorized access or intrusion.
[10] Ann Chen, eWEEK, "*M-Commerce Security a Moving*," January 14, 2001.

The Economic Espionage Act of 1996 provides that it is a federal crime to take, download, receive or possess trade secret information obtained without the owner's authorization. Accordingly, even the online receipt or mere possession of this information which was transmitted through a vulnerable security system could give rise to criminal liability. Upon conviction, a company could be fined no more than $10 million and suffer a government forfeiture of property and computer equipment. Additionally, the National Information Infrastructure Protection Act of 1996 was enacted as part of Public Law 104-294. This Act amended the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, providing for fines and penalties.

D. <u>General Information Practices and Security</u>.

It is essential for companies conducting business or advertising over the internet to establish a privacy policy based upon fair information principles, adequate security and deference to customers' preferences regarding unsolicited e-mail. BBB onLINE, in an article dated August 9, 2000, has published its recommended minimum security standards as follows:

> **Provide Adequate Security:**
>
> On-line advertisers should use appropriate levels of security for the type of information collected, maintained or transferred to third parties and should:
>
> 1. Use **industry standard levels of encryption and authentication** for the transfer or receipt of healthcare information, Social Security numbers, financial transaction information (for example, a credit card number), or other sensitive information,
>
> 2. Provide **industry standard levels of security and integrity** to protect data being maintained by computers, and
>
> 3. **Take reasonable steps to require third parties** involved in fulfilling a customer transaction to **also maintain appropriate levels of security**.

(Emphasis added.)[11]

Therefore, in order to avoid third-party liability, at a minimum, businesses must maintain "*industry standard levels of security*" in order to prove that they provided the requisite standard of care in response to any third-party claim of liability. Clearly, the failure to provide even industry standard levels of security will virtually guarantee a finding of negligence.[12]

III. LEGISLATION AND GOVERNMENTAL ANALYSIS OF SECURITY RISKS

A. The Federal Trade Commission.

The Federal Trade Commission Act, 15 U.S.C. 45(a) prohibits unfair methods of competition and deceptive acts or practices in or affecting commerce. Internet commerce is within the ambit of the statute and subject to Agency regulation.

1. The March 26, 1998 Report. On March 26, 1998, a representative of the Federal Trade Commission ("FTC") presented a report regarding internet privacy to the Subcommittee of Courts and Intellectual Property of the House of Representatives. The Commission's representative informed the Subcommittee that consumers were concerned about the security of their private information on the internet. The FTC representative announced that the Commission had assumed a proactive approach to on-line privacy issues impacting consumers by (i) identifying potential consumer protection issues concerning on-line commercial transactions and marketing endeavors and (ii) providing a public forum for exchange of ideas and (iii) encouraging self-regulation.[13] The Commission was primarily concerned with databases containing consumers' personal identifying information, unsolicited commercial e-mail, on-line

[11] Id.

[12] Recently, Dr. Michael Rabin and his Ph.D. student, Yan Zong Bing, announced the discovery of unbreakable coded messages which cannot be deciphered. This code is based upon a key that vanishes even as it is used. Gina Kolata, Science "*The Key Vanishes: Scientist Outlines Unbreakable Code*," February 20, 2001. This raises the issue of whether *"industry standard levels of security"* require use of unreasonable codes or merely reasonable precautions.

collection information and children's privacy in the on-line environment. The representative reported that the Commission had been instrument in encouraging individual reference services collecting personal data to abide by Individual Reference Services Group ("IRSG") self-regulation. The IRSG principles prohibit distribution of credit reports or information to the general public including Social Security numbers, mothers' maiden names and date of birth. Moreover, consumers will have the ability to access nonpublic information maintained about them in the services and to prevent distribution to the general public. The Commission also encouraged public agencies to institute safeguards to prevent the indiscriminate dissemination of private information. Finally the FTC encouraged individual reference groups to educate the public.

The FTC also developed a recommended policy in protecting the on-line privacy by advising consumers as follows: (i) notice concerning the website's information practices; (ii) choice in how website users will utilize personal information, and (iii) security of consumers' personal information and (iv) the ability to access information.

2. <u>The May 25, 2000 Report</u>. On May 25, 2000, the Chairman of the FTC delivered a prepared statement to the Committee on Commerce, Science and Transportation of the United States Senate entitled "*Privacy On-Line: Fair Information Practices in the Electronic Marketplace.*"[14] The chairman reported that in 1999, retail e-commerce exceed $5.3 billion for the first quarter of the year. A study conducted by the FTC revealed that 92 percent of on-line households reported that they did not trust internet businesses to maintain the confidentiality of their personal information. The report cited the Georgetown Internet Privacy Policy Survey which found that although privacy disclosures were frequent, most internet business fail to

[13] The Commission's report may be found in its entirety at www.ftc.gov/os/1998/9803/privacy.htm.

advise consumers of all four fair information practice principles recommended by the Commission in 1998. An FTC survey conducted in 2000 indicated that 97 percent of internet businesses collected personal identifying information about consumers. As a result of its privacy concerns, the FTC recommended congressional regulation to ensure protection of consumer privacy on-line. The proposed legislation would track to IRSC guidelines, and provide consumers the following rights: (i) clear and conspicuous notice of a website's information practices including what information is collected, how it is utilized, security to consumers and whether this information is disclosed; (ii) providing a choice as to how the personal information is utilized to consumers; (iii) offering consumers reasonable access to information collected about them; and (iv) reasonable steps of the website to protect security of information collected from consumers.

B. Information Infrastructure Task Force.

The White House formed the Information Infrastructure Task Force ("IITF") to create and implement standards for comprehensive technology, telecommunications and information policies. The President's Commission on Critical Infrastructure Protection was the first national effort to address the vulnerabilities of the New Information Age. This Commission was established in 1996 by Presidential Executive Order 13010. The purpose of the Commission was to provide a comprehensive national strategy for protecting the infrastructures from physical and cyber threats.[15]

C. General Accounting Office.

In February 2001, the General Accounting Office provided a report to the Subcommittee on Government Efficiency Financial Management and Inter-Governmental Relations of the

[14] The report in its entirety may be found at www.ftc.gov/os/2000/05/testimonyprivacy.htm

House of Representatives concerning information security. This document focuses upon privacy concerns of governmental agencies and the utilization of confidential and sensitive data collected by the United States Government.

IV. INSURANCE CONSIDERATIONS

A. The Genesis of the Cyber Policy.

1. **Traditional Policies.** Internet commercial transactions and web-based advertising have increased the demand for insurance coverage both for third-party and first-party liabilities.[16] There is currently extensive speculation regarding whether traditional policies extend coverage for destruction of computer data. Such computer virus related losses or damages to computer programs or data may potentially be covered by all-risk policies.[17] The potential liabilities with respect to internet business transactions may not be covered by the typical comprehensive general liability policy ("CGL"). For example, the standard CGL, which restricts coverage to *"bodily injury"* or *"property damage"* defines *property damage* as "(a) *physical injury to tangible property* or (b) *loss of use of tangible property that is not physically injured*." The wrongful or inadvertent dissemination of private information has also been categorized as *"property damage."* In Retail Systems Inc. v. CNA Insurance Co., 469 N.W.2d 735 (Minn. Court of Appeals, 1991) a court has ruled that data constitute tangible

---

[15] See www.iitf.nist.gov; www.pccip.gov.

[16] *See generally* David R. Cohen and Roberta D. Anderson, "*Insurance Coverage for "CyberLosses*," Tort & Insurance Law Journal, Volume 35, No. 4, Summer 2000, pp. 891-927.

[17] An article in the National Law Journal stated:

> "All-risk" policies are the property insurance policies that most likely will cover cases of computer virus related loss or damage to programs or data and cases that result in business interruption. An all-risk policy provides coverage for physical loss or damage to insured property from all perils that the policy does not specifically exclude . . . Moreover, there is a strong argument that all-risk property policies not containing the "destruction, distortion or corruption language" also cover such loss or damage because of the all encompassing nature of the all-risk coverage absent a specific exclusion.

property in the insurance context. Additionally, bodily injury claims could result from viruses or the destruction of medical information resulting in inappropriate medical treatment arguably covering CGL coverage. The National Law Journal speculates that a failure of a computer controlled system to perform properly such as a virus affecting flight control system operations resulting in bodily injury could invoke the coverage provisions of most CGL policies.[18] Many losses, however, may not be within the ambit of most business policies. For example, certain directors and officers liability coverage policies specifically exclude the actual or alleged loss of confidential information of any kind whatsoever including, but not limited to, trade secrets or the actual alleged or anticipated failure of computer equipment.

2. The Cyber Policy. In response to a market niche, cyber policies or network security insurance policy forms have been developed. Generally, network security insurance policies extend coverage for liability coverage, media coverage, coverage for cyber extortion, property loss (both tangible and intangible), criminal reward coverage and coverage for loss of public relations or crises management activities. First-party coverage extends to direct physical loss or damage to covered property and business interruption in the event of service attacks.[19] Additionally, some policies extend protection for computer crime coverage for losses from theft of electronic assets or computer related extortion.[20]

B. Security Evaluations in the Assessment of the Risks.

The adequacy of security standards and attendant risks of a business engaged in internet commerce are the seminal criteria for an underwriter in the evaluation of the assessment of the risk and setting the amount of the premium. Two security consultant corporations are currently

---

Carter, Robert L., The National Law Journal, *Insurance Law: Coverage for Computer Viruses*, June 5, 2000, p. B9.
[18] Id.

working with the London insurance market to reduce the potential security risks and resulting liability for potential assureds. Counterpane Internet Security provides its customers managed security monitoring services for Counterpane's insurance program.[21] Counterpane's managed security services "*eases insurance underwriters' concerns about the level of risk they are taking on*."[22] Similarly, Portland-based Trip Wire, Inc. provides internet security software to reduce the potential of hacker penetration and the vulnerability of customer sensitive data. This service reduces the underwriting risk and certain underwriters have offered a policyholder 10 percent discount on cyber related premiums if a Trip Wire software is utilized as part of the security control. Certain underwriters have accordingly integrated the Trip Wire reports into the policy wording to condition coverage upon maintenance of certain security standards. This policy wording minimizes the risk that an assured's substandard security system will result in a loss to underwriters.[23]

V. CONCLUSION

Corporate security practices are the touchstone for minimizing business losses, third-party liability and potential criminal liability. Moreover, adequate security practices constitute an important consideration for reducing losses, averting a casualty, and providing a tangible basis for underwriters to assess the risk to be undertaken.

---

[19] Professional Liability Underwriting Society Journal, "*Liability Insurers Need to Know How to Deal with Fast Growing Cyber Crime*," January 2001, Vol. XIV No. 1, pp. 6-8.
[20] Susan Breidenbach, Network World, "*Worried About Network Security*," October 23, 2000.
[21] Peter Sayer, Network World Fusion News, "*Lloyd's of London Backs Insurance Against Hacker*," July 10, 2000.
[22] Id.
[23] Shelly Strom, The Business Journal, "*Trip Wire Partners Up with Lloyds of London*," March 2, 2001.