Laptop Data Breaches: Mitigating Risks Through Encryption and Liability Insurance

By Julie Machal-Fulks and Robert J. Scott

SCOTT & SCOTT
COMPLIANCE SIMPLIFIED

SCOTT & SCOTT

COMPLIANCE SIMPLIFIED

Laptop Data Breaches: Mitigating Risks Through Encryption And Liability Insurance

By Julie Machal-Fulks and Robert J. Scott

I. Introduction

Since February 2005, the identities of approximately 93 million people have been exposed because of data leaks.[1] Ponemon Institute conducted a recent survey of almost 500 corporate information technology departments regarding the security risks associated with portable devices, such as laptops, personal data assistants (PDAs) and USB memory sticks. Ponemon reported that 81 percent of respondents have experienced a lost or stolen laptop or portable storage device.[2]

These losses of information can be very costly. According to a report published by Symantec, the average laptop contains data worth approximately $972,000.[3] The Federal Bureau of Investigation Computer Crime Survey estimated that the average annual cost of computer security incidents is $67.2 billion.[4]

Average direct, indirect, and opportunity costs to companies who experienced a data breach was $14 million per company.

A study of the actual costs incurred by companies that lost confidential customer information indicates that the average direct, indirect, and opportunity costs to companies who experienced a data breach was $14 million per company.[5] Companies also saw an average cost of $140 for every customer with breached data.[6] The average number of customers affected by breaches of confidential information was 100,000.[7]

The costs are not only monetary, but can also include loss to business reputation and customer good will. A recent survey indicated that when companies send notice to their customers that their data has been compromised, 19 percent terminate the relationship, 40 percent consider terminating the relationship, and 27 percent are concerned about the relationship.[8] Fifty percent of the costs associated with recovery costs after a data breach are attributable to loss of existing customers.[9]

Businesses and government entities have recently faced intense scrutiny and negative publicity following theft of laptops and other mobile devices. This article will examine some of the details regarding the various thefts and losses and make some general recommendations about how to minimize the organizational impact and negative consequences following a loss.

II. Laptops Lost in 2006

Hundreds of thousands of individuals received notification this year that their personal information was compromised when criminals stole laptops or other portable devices containing sensitive information. This section will describe the facts from some of the prominent cases this year. Many of these cases are recent, and it is unclear what litigation, if any, will result from the data breaches.

General Electric

In early September, a General Electric official left a laptop computer in a locked hotel room. The laptop contained the Social Security numbers of 50,000 current and former employees. The official was authorized to have the data on the laptop. Thieves stole the laptop from the Official's locked hotel room.

Although there was no immediate sign that the information had been used improperly, the personal information on the laptop included all the information necessary to steal someone's identity. General Electric offered one year of free credit monitoring for affected persons.

Ernst & Young

In four separate instances this year, Ernst & Young employees lost laptop computers. The laptops contained sensitive information about hundreds of thousands of Hotels.com customers and Sun Microsystems, IBM, Cisco, BP, and Nokia employees. In the March theft, four Ernst & Young employees left their laptops in a hotel conference room while they went to lunch. When they returned, their laptops, along with the sensitive data contained within, were missing. Ernst & Young claims that as of March 9, 2006, it required all of its employees to encrypt all the data on their laptops.[10]

Fidelity Investments

Fidelity Investments also suffered the embarrassing publicity associated with a data breach when it was required to notify 196,000 current and former HP employees that it lost a laptop. Fidelity indicated that it enacted additional security procedures to prevent unauthorized access to the HP accounts. Fidelity also offered free 12-month credit monitoring for the victims of the data loss.

University of Minnesota

The University of Minnesota instituted a policy in May 2006 regarding breaches of personal information.[11] The University adopted a policy that was designed to "protect[] individuals from potential harm arising from the unauthorized

acquisition of private information about them, and promote[] compliance with state and federal privacy laws."[12] Under the provisions of the new policy, the University is required to provide "timely and appropriate notice to affected individuals when there has been a breach of security of private data about them."[13]

In less than six months, the University reported that several hundred students' personal information was compromised when two Apple computers were stolen from a locked office. Most of the records on the computers did not contain Social Security numbers, but did contain addresses, phone numbers, student IDs, birth dates, citizenship and other personal information.

The Boeing Co.

In April 2006, The Boeing Co. reported that the names, Social Security numbers, addresses and phone numbers of 3,600 current and former employees were compromised after someone stole a human resource employee's laptop at an airport.[14] After the theft, Boeing purged all personal information off of the human resources laptops. Like many of the other companies, Boeing offered free credit reporting for those employees who were affected by the theft. Additionally, Boeing reported that in the future, all the data on laptops will be encrypted, and employees handling sensitive personal information must take participate in special training.[15]

Ameriprise Financial, Inc.

Ameriprise Financial reported a similar breach in January 2006 when thieves stole a company laptop from an employee's car. A file on the laptop contained names, and financial account numbers for 158,000 Ameriprise clients and 68,000 advisers.[16] Ameriprise terminated the employee after learning that, in violation of Ameriprise's policy, the files on the laptop were not properly encrypted.

Government Breaches

Private businesses are not the only victims of theft relating to confidential information. In the largest security breach on record involving Social Security numbers, a U.S. Department of Veteran's Affairs employee violated agency policy and took a laptop containing the sensitive personal information of 26.5 million veterans discharged after 1975.[17] Burglars stole the laptop from the employee's home. The information stolen included names, Social Security numbers, disability ratings, spouses, and dates of birth.[18] In June, veterans filed class-action lawsuits seeking $1,000.00 for each of the 26.5 million people listed in the missing database files.[19]

On a smaller scale, two Federal Trade Commission laptops disappeared from a locked trunk. The FTC attorneys were working on a case, and were authorized to have the laptops. The information on the laptops included the names, addresses, Social Security numbers, financial account information, and dates of birth for persons the FTC had investigated. The laptops did not contain any information about FTC employees or government officials. Ironically, the laptops contained sensitive personal information for defendants that had been investigated for stealing other people's identities. The FTC offered free credit monitoring for 110 people as a result of the theft.

III. Legal Ramifications of Data Theft

For both government and private entities, the cost of the data loss may be significant. In the Veteran's Administration case, the personal information on the employee's laptop was not encrypted and was easily accessible.[20] The two class-action lawsuits currently pending in federal courts are based, in part, on violations of the Privacy Act. The Privacy Act prohibits government agencies from disclosing personal information without the individual's consent. Members of the class can recover not less than $1,000.00 each for the unauthorized disclosure of their personal information.

For both government and private entities, the cost of the data loss may be significant.

Federal Class Action Litigation

On May 30, 2006, Paul Hackett and Matthew Page filed a class action complaint against the Veteran's Administration in the Eastern District of Kentucky. Hackett is a veteran of the United States Marine Corps and Page is a veteran of the United States Navy. The plaintiffs allege that over three years, an unidentified, low-ranking data analyst and long-time VA employee removed files containing private personal information of 26.5 million veterans. The employee then took the files home and copied the files onto his computer for an "unspecified purpose."[21]

The plaintiffs also allege that high-ranking officials at the VA delayed reporting the unauthorized activity until three weeks after the employee reported the laptop stolen.[22] Additionally, the plaintiffs claim that the VA has previously received failing grades for its computer security practices from both the General Accounting Office and the United States House of Representative's Committee on Government Reform. The plaintiffs based their claims on violations of the Privacy Act, and the Fourth and Fifth Amendments to the United States Constitution.

Separate groups of plaintiffs filed the second class action matter on June 6, 2006 in the District Court of Washington, D.C.[23] These plaintiffs claimed that the VA violated the Privacy Act and the Administrative Procedures Act.[24]

State Class Action Litigation

Although the Privacy Act does not apply to private businesses, entities whose data has been breached, like

Ernst & Young and General Electric, must ensure that they comply with the relevant state security breach notification statutes. Twenty-nine states already have security breach notification laws in effect and four additional states have enacted laws that will become effective on January 1, 2007. If a company suspects that its data has been breached, it is critical for the company to determine which state breach notification laws apply to its data breach, and it must comply with the specific terms of each of the notification laws.

In addition to breach notification laws, companies that experience a data loss must also be concerned that the affected individuals will file a civil suit seeking redress for their damages. For instance, a group of plaintiffs filed a class-action lawsuit against Providence Health Systems – Oregon for negligent loss and disclosure of protected health information and for violation of Oregon's Unlawful Trade Practices Act.[25]

In the Providence case, Providence's employee left the office with tape back ups and disks containing more than 365,000 patient records.[26] The employee left the information in the car, where it was stolen. When the patients indicated that they would like Providence to protect them from possible identity theft by providing credit monitoring, Providence refused and suggested that the patients take steps to protect themselves.

Because the information stolen was medical information, plaintiffs claimed that Providence violated the Oregon statute requiring protection of medical information. Plaintiffs further sought damages under the Unlawful Trade Practices Act because Providence represented that it would keep all personal information confidential when it sold medical services and products to the patients.[27]

Regulatory Action

Several companies were recently fined by the Federal Trade Commission for security breaches that resulted in personal information disclosures. Although these security breaches were not directly related to lost hardware like laptops, there is no indication that the FTC would treat a company more leniently because it lost consumer information in a theft while an employee was transporting the data on a portable device.

The FTC has investigated and pursued companies in a variety of industries for breaches of security. The industries include a data collector for credit card companies, a wholesale warehouse retailer, a mortgage company, a national pet store chain, an internet service provider, and a national shoe retailer.[28] In the cases based on breach of security or information, the FTC based its allegations on the following:

- Unfair practices;
- Violations of the Fair Credit Reporting Act;
- Failure to maintain adequate security;
- Failure to protect financial data; and
- Failure to disclose security breaches.

In January 2006, ChoicePoint paid the FTC $10 million in civil penalties and $5 million in consumer redress after ChoicePoint disclosed personal information about 163,000 consumers. At least 800 distinct cases of identity theft resulted from the ChoicePoint disclosure. The FTC claimed that ChoicePoint failed to take reasonable measures to protect company data. Additionally, the FTC alleged that ChoicePoint misrepresented its privacy policies to consumers.

In May, the FTC settled a matter against Nations Title Agency, Inc. Nations Title is a real estate services company operating in 44 states. It routinely collects personal and sensitive information related to home mortgages. The FTC alleged that Nations Title violated the GLBA standards for safeguarding information and the Fair and Accurate Credit Transactions Act Disposal of customer information. The FTC discovered evidence that Nations threw customers' confidential information into the dumpster. To compound matters, hackers accessed Nations' computers and stole sensitive personal and financial information. Like ChoicePoint, the FTC also alleged that Nations made misrepresentations regarding the security of its data.

On September 19, 2006, the FTC outlined several measures identified by the Identity Theft Task Force to help address the increasing problem of identity theft.[29] The Task Force recommends that the government adopt factors regarding "whether and how to give notice to affected individuals in the event of a government agency data breach, and the factors that should be considered in deciding whether to offer services such as free credit monitoring. Such guidance is the first comprehensive road map of the steps that agencies should take to respond to a breach and to mitigate the risk of identity theft."[30] The Task Force also recommended that agencies reduce the access to personal and confidential information and implement policies to increase data security.

Approximately 60 percent of PDAs and 59 percent of laptops contain unprotected sensitive or confidential information.

IV. The New Standard of Care: Data Encryption on Portable Devices

Approximately 60 percent of PDAs and 59 percent of laptops contain unprotected sensitive or confidential information.[31] Almost half of businesses surveyed by the Ponemon Institute indicated that they would never be able to determine the actual information that they lost.[32] There are a number of precautions businesses and their employees should take to ensure that they have met the minimum

standard of care related to protecting sensitive data contained on laptops or other mobile devices. These security measures include:

- Protect information stored on the laptop with a secure password. It should consist of a combination of numbers and upper and lower-case letters.
- Implement advanced security measures such as Remote Laptop Security and laptop encryption.
- Be sure that all important data contained on the laptop is backed up.
- Make use of physical security measures like locks and cables. These security devices make theft more difficult and thereby discourage thieves from taking your machine.
- When leaving a laptop in the office, make sure it is hidden and secured.
- Keep your laptop in an inconspicuous case. Flashy cases expose your computer by attracting thieves' attention. A simple padded messenger bag can suffice as a protective container.
- When using a laptop for meetings or conferences, always keep it in your sight. Do not leave the room without taking the laptop with you.[33]

The Ernst & Young laptop theft in Miami could have been prevented if employees had followed these simple instructions. Furthermore, the companies whose data was stolen could have easily identified the compromised data if the companies regularly backed up the information contained on the laptops. Finally, all of the information could have been protected if it was encrypted. Only 65 percent of the Ponemon survey respondents claimed that their organizations utilize encryption to protect information.[34]

Interestingly, while most organizations that participated in the Ponemon survey indicated that the organization had a response process in place to deal with stolen or lost laptops, the organizations did not have a similar process for lost USB memory sticks.[35] To reduce potential liability related to security breaches, businesses should adopt all-encompassing practices to ensure that it quickly and effectively responds to any potential data loss or exposure.

V. Using Insurance Coverage to Mitigate Risk

Many commercial liability policies do not provide coverage for data security breaches. However, some insurance providers are offering businesses new types of coverage specifically designed to assist with the new risks associated with technology, including costs associated with data breaches. Initially, many corporate identity or security breach insurance policies will defray the costs associated with investigating the breach to determine whether state laws require notification of the breach. Additionally, the insurance coverage will provide assistance to pay for the costs associated with breach notification requirements.

The new policies include coverage for the following claims:

- Failure of network security;
- Wrongful disclosure of private or confidential information;
- Failure to protect confidential or private information; and
- Violations of federal, state, or local privacy statutes.

Many companies face tremendous negative publicity after they experience a data loss or security breach. New corporate identity theft insurance policies will also assist with the costs associated with defraying damage to the company's reputation following a security breach. The insurance coverage will provide crisis management and reimbursement for public relations expenses.

Most importantly, the insurance coverage will provide a defense in the event that a security breach results in a regulatory investigation or a civil lawsuit. For example, AIG's Corporate Identity Protection offers a unique product that covers administrative expenses resulting from an administrative action related to a breach of personal information. Like a traditional commercial policy, the security breach policies contain provisions that the insurance company will be required to pay for an attorney to defend the company in the unfortunate event that the company experiences a data or security breach. Finally, the insurance products also cover the costs post-event services, like credit monitoring and identity theft education, to the individuals affected by the security breach.

VI. Conclusion

Obviously, it is important for companies to protect their valuable data, including the confidential information of their customers and employees. Recent cases have indicated that in the current world of mobile technology, safeguarding data may be difficult. To minimize potential liability, companies should proactively monitor their security policies, encrypt their data, and report breaches as required by state law. Companies should also consider purchasing insurance coverage to protect them in the event that their data is stolen or lost.

Notes

[1] Privacy Rights, A Chronology of Data Breaches, October 7, 2006. Online at www.privacyrights.org/ar/ChronDataBreaches.htm.

[2] Ponemon Institute, LLC, "U.S. Survey: Confidential Data at Risk." 15 Aug. 2006.

[3] Sturgeon, Will, "Could your laptop be worth millions?" C-Net News.com 27 Jan. 2006. Online at http://news.com.com/Could+your+laptop+be+worth+millions/2100-1029_3-6032177.html.

[4] Evers, Joris, "Computer crime costs $67 billion, FBI says" C-Net News.com 19 Jan. 2006. Online at http://news.com.com/Computer+crime+costs+67+billion%2C+FBI+says/2100-7349_3-6028946.html?tag=nl.

[5] PGP Research Report Summary, "What Does a Data Breach Cost Companies." Nov. 2005.

[6] Id.

[7] PGP Research Report Summary, "What Does a Data Breach Cost Companies." Nov. 2005.

[8] PGP Research Report Summary, "National Survey on Data Security Breach Notification." Nov. 2006.

[9] PGP Research Report Summary, "What Does a Data Breach Cost Companies." Nov. 2005.

[10] Author Unknown, "200,000 HP staff exposed as laptop loss party continues." The Register 22 Mar. 2006, Online at www.theregister.co.uk/2006/03/22/fidelity_laptop_hp/

[11] http://process.umn.edu/groups/ppd/documents/policy/SecurityBreach_pol.cfm

[12] Id.

[13] Id.

[14] Chiu, Lisa, "Boeing worker data on stolen laptop." The Seattle Times, 21 April 2006.

[15] Id.

[16] Nobel, Carmen, "Ameriprise Laptop Theft Puts Client Data at Risk." E-week.com, 26 Jan. 2006. Online at http://www.eweek.com/article2/0,1895,1916087,00.asp.

[17] Rash, Wayne "Veterans Sue VA Over Data Loss." E-week.com, 6 June 2006. Online at http://www.eweek.com/article2/0,1895,1972946,00.asp.

[18] Id.

[19] Id.

[20] Rash, Wayne "Veterans Sue VA Over Data Loss." E-week.com, 6 June 2006. Online at http://www.eweek.com/article2/0,1895,1972946,00.asp.

[21] Hackett, et al. v. United States Dep't of Veterans Affairs, et al. No. 06-114-WOB (E.D. Ky. 2006) Complaint at p. 5.

[22] Hackett, et al. v. United States Dep't of Veterans Affairs, et al. No. 06-114-WOB (E.D. Ky. 2006) Complaint at p. 6.

[23] Vietnam Veterans of America, Inc., et al. v. Nicholson, et al. No. 1:06-cv-01038-JR (D. D.C. 2006), Complaint at p. 1.

[24] Vietnam Veterans of America, Inc., et al. v. Nicholson, et al. No. 1:06-cv-01038-JR (D. D.C. 2006), Complaint at pp. 13-14.

[25] Gibson, et al. v. Providence Health Systems-Oregon No. 0601-01059 (Cir. Ct. Multnomah Co. 2006) Complaint at p. 1.

[26] Gibson, et al. v. Providence Health Systems-Oregon No. 0601-01059 (Cir. Ct. Multnomah Co. 2006) Complaint at p. 2.

[27] Gibson, et al. v. Providence Health Systems-Oregon No. 0601-01059 (Cir. Ct. Multnomah Co. 2006) Complaint at pp. 9-10.

[28] For a detailed discussion of the recent FTC investigations and settlements, see Scott, Robert "Privacy, Network Security, and the Law." IT Compliance Journal, Spring 2006 Vol. 1.

[29] http://www.ftc.gov/opa/2006/09/idtheft.htm

[30] http://www.ftc.gov/opa/2006/09/idtheft.htm

[31] Ponemon Institute, LLC, U.S. Survey: Confidential Data at Risk, August 15, 2006.

[32] Id.

[33] http://en.wikipedia.org/wiki/Laptop_theft

[34] Ponemon Institute, LLC, U.S. Survey: Confidential Data at Risk, August 15, 2006.

[35] Id.

SCOTT & SCOTT

COMPLIANCE SIMPLIFIED

2200 Ross Avenue :: Suite 5350 East :: Dallas, Texas 75201 :: t 800.596.6176 :: f 800.529.3292 :: scottandscottllp.com