LAPTOP THEFT: A GROWING CONCERN FOR ORGANIZATIONS

Robert Behling, Arrowrock Technologies, rbehling@hotmail
Wallace Wood, Bryant University, wwood@bryant.edu

ABSTRACT

This paper examines the growing problem of laptop theft and security. A review of the professional literature was done to determine the magnitude of the problem and what organizations are doing to address it. A survey was constructed and administered to a sample of employees of organizations in southern New England to determine the rate of adoption of security measures by their organizations taken to address this problem. The results of the survey indicated that these organizations primarily used only the most fundamental security measures, use of more sophisticated measures was limited, and one-third of the organizations did no formal training of laptop users.

Keywords: Laptop theft, laptop security, security measures

INTRODUCTION

Laptop computers allow users the same computing capacity and software as many desktop systems. Mobile by design, laptops present increased exposures, risks and challenges for organizations. Unfortunately, those characteristics that make laptops so attractive also make them more prone to theft. Lower laptop prices, user desire for portability, flexibility provided through wireless communication, and increased storage and processing power make laptops very attractive for every business person from the salesman or saleswoman on the road to the CEO visiting company facilities. A mobile workforce supported by laptop computers expands business opportunities, but also presents a security nightmare. Laptop computers are easy to conceal, find a ready used market, and have the capacity to store enough sensitive data to severely damage a company if they are stolen and the data is misused. Hundreds of thousands of business laptop computers are stolen each year from all levels within the organization. There is even a case of a laptop being stolen from a podium during a break in a presentation by the CEO of Qualcom. The real loss was that the laptop contained some very sensitive and strategic business data, as well as the text for the presentation [16].

The use of laptops is clearly on the rise. Intel estimates the number of laptops has doubled between 2001 and 2004 [9], and Dell claims laptop sales growth to be 30% per year [8]. It is projected that by the year 2008 50% of the PC's used in the United States will be laptops [4]. This increase in laptop use comes at a price. A recent CSI/FBI Computer Crime and Security Survey found that laptop theft ranked third for computer crime based on financial losses. Average loss per laptop theft (including remedies for protecting/recovering/safeguarding compromised data) is estimated to be in excess of $30,000 per incident [6].

A stolen laptop is not just an IT issue. When the stolen laptop contains confidential data the theft affects the customer base, customer trust, and the image of the organization [14]. Organizations often focus their security efforts on protecting data from network penetration, hackers, virus disruption and other attacks on their main processing and storage hardware. With the rise in laptop use and theft organizations need to expand security efforts to include policies for laptop security.

Laptop Exposures

Laptops are mobile by design, therefore more vulnerable to theft. It is thought that as many as 80% of all laptop thefts are committed by internal employees, creating a serious human resources issue [12]. Organizations are starting to impose restrictions on who can remove confidential data from their office, and are implementing special training programs to instruct employees in methods of securing data on laptops. These efforts are resulting in more comprehensive data and hardware security practices and policies, and workers found violating these policies are subject to discipline or dismissal [13].

The data stored on a laptop is the greatest liability for an organization. When a laptop is stolen, the data value is much higher than the hardware value. The original intent of the theft may be for resale of the laptop, not theft of the data, but the exposure for misuse of the data remains. Most laptops have insufficient data protection [2], and whether stolen for the hardware or the sensitive data contained in the

laptop storage devices, the organization is subject to exposure to serious financial loss.

Laptop Risks

Recent publicized theft or loss of laptops containing significant sensitive data include the U.S. Department of Veterans Affairs, Fidelity Investments, Electronic Data Systems and Ernst & Young [7]. Along with bad publicity and embarrassment, these and other organizations exposing and losing sensitive customer data face significant financial losses should customers decide to sue. It is interesting to note that most corporations acknowledge the problem, but more than two thirds of them still have not implemented specific laptop security policies [1].

It is estimated that more than 600,000 laptops are stolen each year in the US [5], with more than 93 million data records compromised, putting millions of Americans at risk for identity theft [17]. The majority of laptops are stolen for the hardware value [3], but it is estimated that 10-15% of laptop thieves target the sensitive data stored on the laptop [16]. The loss of a few thousand dollars worth of laptop hardware is modest compared to the financial exposure and damage to a company's reputation that can result from a security breach associated with a laptop theft [18].

Organizational Challenges

Changes in data privacy regulations in the past few years have put pressure on organizations to pay attention to laptop theft. Thirty two states have adopted legislation requiring companies to notify victims when personal information has been lost or compromised [13]. In recent years there has been increasing pressure from the government on organizations to comply with data privacy laws or be held accountable for lost or stolen data [5]. The Privacy Rights Clearinghouse is calling for a national law requiring organizations to directly notify anyone affected by a data breach, be it stolen laptop of hacker infiltration [15].

What can organizations do to better protect against laptop theft and subsequent compromising of data? The most obvious and least expensive method is to provide more enhanced physical security. This would include lock boxes, tie downs, hardware locator devices attached to laptops, and employee searches when leaving the premises. Some organizations are expanding this physical security approach to include restricting employees from taking laptops to specific countries where danger of theft is high, and discouraging or restricting what data can be stored on a laptop [4].

The second protective measure would be to provide better security for the data stored in the laptop. This would include encryption schemes and protecting data access through more effective passwords, biometrics, and other access controls [6]. Data encryption, protection of flash drives, and laptop tracking systems are also being used to safeguard both hardware and data [10].

Organizations are recognizing that employees are the weakest security link [11]. Employee training and increasing the security consciousness of employees, along with a clearly articulated laptop policy statement outlining an employee's responsibilities can reduce the risk of theft by increasing the employee's awareness [16].

A laptop security policy statement might include items such as:

Responsibility of Users

- The user should take responsibility for the security of the laptop and stored information
- The user should take precautions to protect against the installation of malicious software
- The user should insure proper care is taken of the laptop

Physical Security

- The laptop should not be left unattended in public places
- Sensitive information should not be displayed on the laptop in public places
- Laptops should be carried as hand luggage when traveling

Access Control

- All data on the laptop should be encrypted
- All sensitive data should be periodically backed up

Laptop Loss

- If the laptop is stolen or lost it should be reported to the authorities immediately

(adapted from: Narasimman, "Laptop Security", www.securitydocs.com/library/3399)

Some organizations are now looking to outsourcing their cyber security needs, including laptop theft protection. Organizations also have the option of obtaining cyber insurance to help mitigate risks. These are relatively new approaches, and may offer protection and risk mitigation, but they are expensive and require management support if they are to be effective.

RESEARCH METHODOLOGY

A survey was designed to determine employee laptop computer use and organizational security measures for such employee use. After reviewing the literature on security measures employed by organizations to prevent the loss of data on laptop computers as well as the computers, an initial survey was constructed. This survey was tested on a select sample and revised to reflect the suggestions and comments from the respondents. The survey consisted of three parts: 1) Demographics of the respondents' companies/ organizations; 2) IT security policies and procedures in place at the respondents' organization; and 3) Specific information related to the use and theft of laptop computer equipment.

The survey was administered to graduate students in a northeastern university Masters of Business Administration (MBA) program who were employed full-time in businesses and organizations in southern New England. After removing responses from duplicate organizations, the sample size was 62.

SURVEY RESULTS AND DISCUSSION

As can be seen from Table 1, 50 of the 62 organizations (81 percent) of the companies in the sample provide laptop computers to at least some of their employees. Thirty six of the respondents indicated they were provided a company laptop computer. It is the responses from these employees which are used in the following discussion and tables.

Table 2 summarizes how the laptops are used by the respondent employees with respect to access to corporate data, where they are used, and whether users are given training on the security of the laptops. Of interest is that 100% of the respondents had laptop access to company data at remote sites, including their home, and 78% were allowed to store company data on their laptop. This indicates that for at least this sample, there may be significant exposure to the loss of sensitive and valuable data stored on company laptops. Security awareness can be emphasized through training, yet 36% of the organizations do not provide such training.

Table 3 lists possible security measures that organizations can implement and how many organizations represented in the sample actually use one or more of these measures. Of the 15 security measures listed, only 3 of them have been adopted by over 50 percent of the companies sampled. As expected, password protection with a 97 percent adoption rate is the number one security measure, but data encryption with a 56 percent adoption rate is disappointing as is the 56 percent adoption rate for employee certification/signoff. Despite the fact that the literature lists many possible security measures/devices, the organizations in this sample for the most part adopted them at a very low rates.

Table 1
Size of Organization
vs.
Provide Laptops to Employees

Number of Employees	Organization Provides Laptops to at Least Some Employees	
	Yes	No
1- 50	4	6
51- 500	6	5
501- 2,000	8	1
2001- 10,000	16	0
Over 10,000	16	0
	50	12

Table 2
Using the Company Laptop
N=36 Respondents

	Number (%)of Responses	
	Yes	**No**
Use laptop to access company data in the office?	**35 (97)**	**1 (3)**
Use laptop to access company data at remote site?	**36 (100)**	**0 (0)**
Take laptop home on a regular basis?	**36 (100)**	**0 (0)**
Store company data on the laptop?	**28 (78)**	**8 (12)**
Take the laptop on business trips?	**33 (92)**	**3 (8)**
Organization provides training on security of the laptop?	**23 (64)**	**13 (36)**

Table 3
Which of the following security measures
for laptops is in place in your organization?
N = 36 respondents
Multiple Responses Possible

	Number of Organizations	Percentage of Organizations
Passwords	**35**	**97**
Encryption of data	**20**	**56**
Employee certification/signoff	**20**	**56**
Awareness training	**16**	**44**
Locking cables	**13**	**36**
Data restriction on laptop	**13**	**36**
Automatic encryption of data	**12**	**33**
Internet tracking/locator software	**9**	**25**
Smart cards	**7**	**19**
Key cards	**7**	**19**
Deletion programs	**4**	**11**
Biometric access controls	**4**	**11**
Kensington locks	**2**	**6**
Motion sensors and alarms	**1**	**3**
Travel prohibitions	**1**	**3**
Unknown	**1**	**3**
Others	**0**	**0**

CONCLUSIONS

The theft of laptop computers is a growing problem faced by businesses and organizations. These thefts are not only a problem because of the financial costs of the computers and software, but more importantly because of the organizational and personal data contained on them. While most laptops are stolen for the value of the computer, a significant number are taken to gain access to sensitive information and company information stored on the laptop. This presents a significant risk to business organizations that allow their employees to store company data on their laptops.

The results of a survey of business professionals employed by organizations in southern New England revealed that for the most part these organizations used only the fundamental security measures of password protection, data encryption, and employee certification to mitigate the risks from lost or stolen laptops and their stored corporate data. There was limited use of more sophisticated security measures such as tracking and biometrics. Perhaps the most disappointing outcome from the survey was the reported limited security training, with only two thirds of the organizations providing security training for employees utilizing company laptops.

REFERENCES

1. _____. (2006). "PC Theft Recovery Statistics," Retrieved March 4, 2007 from http://www.absolute.com/Public/main/aptop-theft-statistics.asp.
2. ____ (2006) "Stay Out of the Headlines – The Next Generation of Encryption for Notebooks, Tables, and Desktops," Credant Technologies White Paper, Retrieved March 4, 2007 from http://www.computerworld.com/pdfs/Credant _White_Paper.pdf.
3. Anthony, B. (2006). "The Laptop Dilemma: When Sensitive Data is Snatched," Document Processing Technology, August, V. 14, N. 5, p. 7.
4. Fitzgerald, M. (2004). "How to Stop a Laptop Thief," CSO Career Email Newsletter, Retrieved March 4, 2007 from http://www.csoonline.com/ read/070104/laptop.html.
5. Ganapati, G. (2006). "Got Laptop Security?" Red Herring, August 14, Retrieved March 4, 2007 from http://www.redherring.com/article.aspx?a= 17953&hed=Got+Laptop+Security?&sector= Industries&subsector=Computing#.
6. Gordon, L, Leeds, M, Lucyshyn, W. and R. Richardson. (2006). "2006 CSI/FBI Computer Crime and Security Survey," Retrieved March 4, 2007 from http://www.cmpnet.com/gocsi/ db_ area/ pdfs/fbi/FBI2006.pdf.
7. Greenwald, J. (2006). "Laptop Theft wave Exposes Liability," Business Insurance, June 19, V. 40, N. 25, p. 1.
8. Kessler, M. (2005). "Roaring Laptop Sales Boost PC Market," Retrieved March 4, 2006 from http://www.usatoday.com/tech/news/2005-01-23-laptop_x.htm.
9. Lemon, S. (2003). "Laptop Sales to Outpace Analysts Prediction, Intel Says," InfoWorld, October 21, Retrieved March 5, 2007 from http://search.infoworld.com/query.html?qt= Laptop+Sales&charset=utf-8&ht=0&qp= &qs=&qc= &pw=100%25&ws=0&la= en&qm= 0&st=1&nh=10&lk=1&rf=1&rq=0&si=0
10. Lendino, J. (2005). "Secure Your Laptop's Data," Retrieved March 4, 2007 from http://www.cnet.com/4520-10192_1-6389240-1.html.
11. Litan, A., Mogull, J. and J. Girard. (2006), "Stolen FTC Laptops Show Extent of Lax Security Practices," Retrieved March 4, 2006 from http://www.Gartner.com, ID # G00141697.
12. Livingston, J. (2006). "Don't Lose Your Laptop," Retrieved March 4, 2007 from http:// www.smartbiz.com/article/view/1506/1/59.
13. McQueen, M. (2006). "Laptop Lockdown: Companies Start Holding Employees Responsible for Security of Portable Devices They Use for Work," The Wall Street Journal, June 28, Retrieved March 4, 2007 from http://online.wsj.com/page/ppv_snippet-SB115145402822192505-search.html.
14. Quinn, O. (2006). "How to Avoid Laptop Lapses: Your Notebook's Lost or Stolen. Now What?," National Post, Don Mills, Ont, August 2, p. WK.1.
15. Regan, K. (2006). "Laptop Thefts Accelerate Data Privacy Concerns," eCommerce Times, June 23, Retrieved March 4, 2007 from http://www.ecommercetimes.com/story/51326.html.
16. Ryder, J. (2001). "Laptop Security, Part One: Preventing Laptop Theft," Retrieved March 4, 2007 from http://www.securityfocus.com/ print/ infocus/1186.
17. Schwartz, J. (2006). "Companies Take Costly Steps to Secure Laptops," USA Today, July 23, Retrieved March 4, 2007 from http:// www.usatoday.com/tech/news/computer security/2006-07-23-laptop-secure_x.htm?POE = click-refer.

18. Wood, L. (2006). "Technology for Rescuing Stolen Laptops Emerges," ComputerWorld, August 10, Retrieved March 4, 2007 from http:// www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9002333&pageNumber=1.