InformationShield

Information Security Policy Concerns for Laptops and Portable Devices

By David J. Lineman

Privacy breaches dominate the headlines

In just the first few months of 2006, another series of privacy breaches involving lost or stolen laptops exposed the personal information of hundreds of thousands of individuals. Some of the recent high-profile examples:

- In April 2006 Aetna Insurance acknowledged that a laptop computer stolen from an employee's car contained personal data belonging to approximately 38,000 members.
- In March 2006 Fidelity Investments announced it is notifying nearly 200,000 Hewlett-Packard (HP) employees that their account information, including names, addresses and Social Security numbers, was on a stolen laptop.
- In March 2006 Ernst & Young announced that a laptop computer stolen from an employee's car contains sensitive personal data belonging to thousands of current and former IBM employees.

Policies and portable devices

While an obvious technical solution would be the encryption of all data on portable devices, these breaches point to a number of related issues that should be addressed within information security and privacy policies. As we often see, having one security control in place is not effective when one or more other controls have failed. All organizations can learn from these examples by taking a look at their own policies and procedures and identifying weaknesses that may leave them vulnerable.

Data Classification and Labeling

A common policy weakness is in the proper identification and labeling of sensitive personal information. The first link in the chain of protection is to have a data classification and labeling policy that has an appropriate category for private data on employees and customers. In all but the rarest cases, customer and employee

personal data should have a high sensitivity and be subject to stringent organizational controls. A common sensitivity label for this data is “PRIVATE”, indicating that it applies to personal data that is intended only for use within the company.

Many organizations still do not have defined classification schemes that are applied throughout the organization. Even when classification systems exist, users must be trained to properly identify sensitive data (like personal information on customers). Furthermore, data owners should be identified with the responsibility of labeling sensitive data documented in security policies.

Question: Do we have data classification policies that allow for proper labeling of sensitive customer and employee information? Are the appropriate users trained to recognize and/or label this data?

Transmission and Copying of Sensitive Data

A second critical policy control is the restriction of moving, copying or transporting sensitive data without proper controls. In the world of portable computing devices like laptops and PDA’s, is it easy for employees to make copies of sensitive data for work at home or on the road. Sensitivity labels should stay with the data as it moves throughout the organization, especially as it changes media format from print to digital and back again.

Question: Do we have policies that limit the copying, storage and transmission of sensitive data? Do our policies define security controls for various types of media?

Standards for Protecting Portable Devices

Another critical information security policy establishes the link between the sensitive data and the controls required to protect it in various formats. Information security policies should specify that security controls on various hardware and software systems establish protection for the highest sensitivity data that is stored on those systems. In the breach examples, laptops containing customer data should have a high level of protection, including encryption of the data.

The information security department should define a standard set of controls and technologies that are required for any laptop or portable device that may contain sensitive data. Information security policies should document the requirement of information security (or other IT group) to establish these standards and for users to recognize and use these standards.

Despite numerous technical solutions for encrypting data on laptops and other portable devices, many organizations still allow data to leave the organization unencrypted. A 2005 survey of organizations by information security firm Credant Technologies suggests that as many as 90% of laptops lost or stolen from organizations contain some form of sensitive corporate data, and that less than 25% of missing laptops met encryption data requirements mandated by California SB 1386 and other states' breach notification laws.

Question: Do your "Acceptable Use" policies for end-users address the storage and removal of sensitive data on laptops and other portable computers?

Security Education and Awareness

The final link in the chain of policy controls is the requirement for user education and awareness. A common control weakness is that organizations have policies in place, but users are not aware of them or trained to follow them. According to public statements by the company, the employee of Aetna insurance was "not following corporate policy." While this seems like a failure of the employee, further investigation would be required to determine if it was not a failure of the organization to communicate and educate employees.

Security education and training is the vital link in all information security policies. However, it is still one of the most under funded and informal aspects of many information security programs. Information security policies should clearly define the requirements for security awareness and training, as well the organizational roles responsible for planning and executing this training.

Question: Do our information security policies require security awareness training at least once a year for all users?

Resources for Information Security Policies

Organizations that answered "no" to any of these questions may be at risk of exposing sensitive data on a lost or stolen portable computer. Having a consistent set of policies that define the proper controls for identifying, labeling and handling sensitive data is the first step. Next, policies must define how sensitive data is protected as it moved within and out of the organization. Policies must also define the acceptable use of portable devices, including the required security controls for all computers storing sensitive information. Finally, users must be made aware of these policies, with this organizational responsibility clearly stated.

Information Security Policies Made Easy by Charles Cresson Wood, CISSP, CISM provides over 1300 pre-written information security policies addressing each of these topics and many more.