Ernst Enterprises Newsletter

IT HAPPENS: CONFIDENTIAL OR PERSONAL DATA DOES GET LOST OR STOLEN

. . . . . .

A recent bulletin from the law firm of Seyfarth Shaw reported the theft of a laptop from the home of a UK company employee. The laptop contained personal information for about 24,000 clients. Subsequently, the company was fined £60,000[1] (approximately $94,669), demonstrating how serious government regulation is becoming with regard to consumer data and protection of that data.

Current U.S. federal laws include HIPAA (health information), GLB (financial information) and COPPA (children's information), and the recently introduced, but not yet enacted, Data Security and Breach Notification Act of 2010 requires security measures related to personal information. States are also getting into the data protection business too: for example, Massachusetts law now protects its resident's social security numbers.

Do your IT policies answer these security questions?

- What data do you collect and from whom? (customers, employees, others)
- Who in the company has access to the data?
- What methods are in place to protect the data, prevent it from unauthorized viewing and downoading?
- What data must be encrypted and what encryption method is to be used?
- Who is responsible for ensuring legal compliance with these complex regulations?
- What must you do if the data is lost or accessed by an unauthorized person or hacked?
- Who is authorized to do regular software updates?
- Who can upload software into your system?
- Where is your data stored and how is it backed up?
- What is done to clean outdated equipment?

THE 3 STEPS TO AVOID LOSS/THEFT OF PERSONAL DATA

Step 1: Assess your current policies, procedures and practices.
This may sound simple, however most mid-size companies do **not** have up-to-date policies and procedures that address some of the key questions above. Policies and procedures are your first line of defense should a data breach occur: they instruct all employees on what they can and cannot do with regard to your systems and data. Without current policies and procedures you are at greater risk of legal exposure for failing to protect data. Policies are needed to determine who owns the systems and data, under what conditions employees may access and use information stored on the system, publish and/or download private and/or confidential company information, etc.

Step 2: Assess your IT employees.
Assess your IT employees to determine if they know what is legally required to protect data on your systems and if that protection is in place. Many IT employees in mid-sized companies are technical and know how to install a system, conduct repairs, install software, etc, but don't have the in-depth knowledge of or ability to keep up with legal requirements, system upgrades to protect information, or assess systems for growth and increased efficiencies. Frequently companies have different systems installed that don't share information, creating duplication and errors.

When was the last time your IT person attended a seminar or workshop on legal requirements or new system tools? If the answer is never or not in the past few years the likelihood is that their knowledge and skills are out of date.

Step 3: Assess your systems.
We often find a gap between what **should** be on your systems and what **is** on your systems. All applications must be both up to date on "patches" and must be capable of understanding privacy issues. Backup and disaster recovery devices must be considered with an eye to possible disclosure and tested to be sure they work and that you can in fact recover your data.

TELLTALE SIGNS

Do your employees' use company laptops? Do employees use their own laptops or smart phones that store your data? ***If so your company is just as responsible for the data that resides on the laptop as it is for the data that resides on the servers***. Extra security practices need to be in place to protect these portable devices i.e. strong passwords and regular changing of passwords reduce the risk of systems being hacked.

Call Dawn Bremer today at 847/456-6334 to schedule your IT assessment. We have the expertise and experience to assess your IT policies, practices, and employee competence.

- How secure are your systems? Take our systems security quiz to learn more.

- To read more, see Newsletters. Follow us on our new blog, Be a Better Manager.

- What keeps entrepreneurs up at night? Take our newest SURVEY and see how you compare.

[1] Seyfarth Shaw Attorneys LLP, One Minute Memo, November 29, 2010.

Sincerely,

Mark

Mark Ernst
Ernst Enterprises, LLC

EE Ernst Enterprises, LLC