Technology Now
Timely Topics for Academic Medical Centers
a product of the AAMC's Group on Information Resources (GIR)

Group on
Information Resources
GIR

AAMC

Full Disk Encryption of Laptops (Macs and PCs)

January 2011

By Juany Jardines, Memorial Sloan-Kettering Cancer Center; William Barnett, Indiana University

Definition: Technology used to encrypt all data that is written to the hard drive of any computer. It is primarily used on laptops since they are more likely to be lost or stolen. Data on an encrypted drive is not readable by unauthorized users.

Products: PGP Whole Disk Encryption, McAfee Endpoint Encryption, Check Point (formerly Pointsec) Full Disk Encryption. There are many more products on the market but these are the most popular.

Advantages: Improves security, complies with regulations (HIPAA, HITECH, SOX), protects intellectual property, is easy to use (only password required), does not affect workflow.

Disadvantages: Slows down the laptop, adds complexity to trouble shooting and support of the laptop.

Strategic Considerations:

- Choose a single product that will work with the various laptop Operating Systems in your organization. All the products presented here support both Mac and PC laptops.
- Ensure your product choice meets your regulatory requirements.
- Ensure integration with existing authentication methods, Active Directory or others
- Consider not only cost of the product but also support costs.
- Ensure that your support group is prepared to work with the encrypted laptops

Obstacles to Encryption:

These are issues that will be encountered during the implementation process.

Arguments from Users:

- *"My laptop will be too slow"*

Overhead and impact on performance is approximately 10-15%. Most users do not notice the change.

- *"I already encrypt using file/folder encryption"*

Users may not always place sensitive file in the encrypted folder. It will be very difficult to prove that a particular file or folder is encrypted. This will not be the case with Full Disk Encryption.

- *"I don't have sensitive data on my laptop"*

Users are not always aware of what is "sensitive" data.

Implementation Issues:

- Locating and scheduling laptops to be encrypted can be time consuming & difficult
- Encryption may take a very long time especially with bigger drives
- In case of failure during encryption data may be lost, always backup the drive
- Encrypted laptops add complexity and time to technical support

Addressing these issues and arguments before the start of the project will improve odds of success.

Resource links:

https://www.aamc.org/download/108258/data/encryptionreport.pdf.pdf
http://www.ama-assn.org/ama1/pub/upload/mm/368/hipaa-phi-encryption.pdf
http://en.wikipedia.org/wiki/Full_disk_encryption
http://www.checkpoint.com
http://www.pgp.com
http://www.mcafee.com