Thinking About Whole Disk Encryption (WDE)? Some Things to Think About

A growing number of institutions are diligently striving to prevent data breaches involving personally identifiable information (PII), particularly incidents involving the loss of laptops or other mobile devices. While it may never be possible to completely prevent the loss of laptops or other mobile devices, use of whole disk encryption (WDE) may go far to mitigate or minimize the consequences when such incidents when they do occur.

If your site is concerned about potential unauthorized PII disclosure, and you're considering deploying an institution-wide whole disk encryption program, are there any considerations you should keep in mind when doing so? We think so…

1. Be Realistic: Whole Disk Encryption Won't Be Adopted Spontaneously… If you believe whole disk encryption is an important security measure, you should aggressively promote (or require) its use. Do not assume that your users will spontaneously adopt whole disk encryption without official encouragement (or an explicit policy mandate) that it be used.

2. Strong Encryption *Is* Strong! When you encrypt a device with strong encryption, if the password is lost or forgotten, don't assume that you will somehow be able to miraculously "reset" or "overcome" that encryption and recover the encrypted contents – you won't (if you could, so could the bad guys!) Just like using a power tool or firearm, you can hurt yourself if you're careless when you're using strong encryption.

3. Compelling Institutional Interests May Necessitate Password Escrow: If critical institutional data is protected by whole disk encryption, what will the institution do if the person who encrypted that data leaves, dies, or becomes incapacitated? Some whole disk encryption products may make it possible for the institution to "escrow" individual user passwords, or allow use of a "master password" as an alternative to the normal user password.

4. Recognized That Whole Disk Encryption *Can* Potentially Catastrophically Fail: There have been occasions when whole disk encryption has failed in ways which have resulted in the contents of encrypted drives being irretrievably lost.* You may be able to minimize this risk by periodically backing up an image of the encrypted drive, or by archiving an unencrypted copy of the data (but if you do, be sure those unencrypted archives are carefully protected from unauthorized access!)

5. Whole Disk Encryption Won't Protect Against "Social Engineering," "Rubber Hose Cryptography," or Surreptitious Use of Hardware Key Loggers:** If users voluntarily disclose their password after being tricked by a miscreant, or are physically or legally compelled to disclose their password, or their encryption key is captured by a hardware key logger while they're entering it, obviously whole disk encryption won't protect the data on that device.

6. Understand What You Are (and Are Not!) Encrypting: Some encryption products (such as Mac OS X File Vault) may only encrypt particular directories or selected file systems, and not actually encrypt the entire disk. Depending on your requirements, this may be all you need, or a big (and bad) surprise! For example, does swap space get encrypted by the product you're using?

7. When The System's Running, At Least Some Information Won't Be Fully Encrypted: The system can't run if the disk remains fully and continually encrypted. Thus, when it's time to actually use the system, at least some part of the disk will be decrypted/accessible. Given that reality, do users fully power their systems down when they aren't actively using them? Or do they leave them in some other state (such as "sleep" mode), where the content of the disk may potentially not be encrypted? Train users to power down systems completely and properly before travel or storing a WDE protected system!

8. Some Whole Disk Encryption Solutions May Impact System Performance: Don't be surprised if some whole disk encryption solutions impact system performance. In most cases the performance hit won't be enough to preclude use of whole disk encryption, but in some cases you may want to consider deploying faster systems (or systems with more memory) than you otherwise might as part of deploying WDE.

9. Laptops And Other Mobile Devices May Not Be The Only Devices Needing Whole Disk Encryption: For example, how long would it take you to crack the case on a desktop system and pull a hard drive from it? Maybe it should be running WDE, too? And what about the sensitive files on that 16GB or 32GB USB "thumb drives" (or other removable media)? Will the solution you select work on all platforms in use at your site?

10. WDE May Not Completely Eliminate Your PII Breach Disclosure Obligations: While many state PII breach notification laws offer a "safe harbor" exclusion for systems that use WDE, some do not. Be sure you accurately understand what legal protection WDE offers.

11. WDE Won't Protect Your Data When It's Being Sent Over The Wire: While whole disk encryption protects your data when it's at rest on disk, it won't protect it while it's being sent over the network. Ensure you also use strong encryption (such as ssh, ssl, or an IPsec VPN) to protect sensitive data while it's being transferred to and from a WDE-protected device.

12. Not All Whole Disk Encryption Products Are Free/Open Source: While some popular whole disk encryption products (such as TrueCrypt***) are free/open source products, others are commercial software. Don't forget to budget for the cost of whatever product you decide to adopt!

---

* https://pgp.custhelp.com/app/answers/detail/a_id/2288
** http://www.xkcd.org/538/
*** http://www.truecrypt.org/