Implementing Encryption for Stored Data

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

One of my graduate students wrote to me recently about the rash of data losses on unencrypted laptop computers and backup media and asked how I would promulgate policy to cope with the problem. Here’s how I would approach the organizational behavior change needed to ensure that sensitive data on all storage media in the organization.

(a) Establish and implement a company-wide policy forcing encryption of all sensitive folders on company computers, servers and removable media. The policy can use whole-disk encryption (e.g., Encryption Anywhere Hard Disk <http://www.guardianedge.com/products/Encryption_Anywhere/Hard_Disk.html> from GuardianEdge or PGP Corporation’s PGP Whole Disk Encryption products <http://www.pgp.com/products/wholediskencryption/index.html>) or it can focus on partition- or folder-specific encryption. Regardless of which technique or product is used, the organization must plan for key escrow to permit data recovery if an employee forgets a key, quits in anger or is fired. Appropriate products include centralized key management and key-recovery features. Policies must take into account the likelihood that keys and even the encryption software will change over time; therefore, archive managers must manage backups so that data can be recovered and rewritten under the new encryption procedures as they change.

(b) In your IT or IT-security newsletters, publicize the news about the losses of control over unencrypted data on laptop computers, isolated hard drives and tapes. Some employees who do not understand or believe that encryption is important will resist change and may even obstruct progress towards the new procedures. Setting the stage for policy development and implementation helps to smooth the way for change.

(c) Provide extensive awareness, training and education over the next few months for all staff on how and why to follow the encryption procedures for their disks and removable media; be sure to have the employees work on scenarios of what might happen to THEIR group if confidential data were released through loss or theft. Have the technical support staff test the product thoroughly and work on problems likely to occur with the product. You can save a lot of time by recording narrated PowerPoint files that can help users with step-by-step illustrations of what to do with the products; be sure to include screen shots. I often create animations using overlays of screen shots so that users can follow the operations click-by-click.

(d) Begin a gentle process of random audits with praise and reward for those found to be following the encryption guidelines and gentle reminders to those violating the policy. Praise works better than punishment in modifying behavior. Establish friendly competitions among groups to see which can be first to achieve 100% compliance with the encryption regime.

(e) Tighten the screws gradually by announcing the steady increase in penalties for violating the policy; over the next months, bring them to their managers for discussions of the importance of the policy and the future penalties for noncompliance.

(f) After enough time has passed (say, a few months) to ensure almost complete compliance with
the policy, suspend or eventually fire anyone found to be violating this policy during random audits of laptops. However, you will have to be prepared to deal with top executives who violate the policy, so you might want to be careful about promulgating draconian penalties that you don’t plan to enforce uniformly.

[Disclaimer: I have no financial interest in the products named; mention of specific products does not imply endorsement.]

* * *


M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance <http://www.msia.norwich.edu> at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2006 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.