How to Manage Encryption on Windows, UNIX, and Mainframes

(A simple guide for CIOs, CISOs, Security Admins, and Auditors)

Stu Henderson
The Henderson Group
5702 Newington Road
Bethesda, MD 20816
(301) 229-7187
www.stuhenderson.com

Abstract:

This document shows you how to manage the encryption of sensitive information in your enterprise. It does not show you how to encrypt; rather how to assess, improve, and demonstrate that your encryption program is effective. Whether you are a CIO, CISO, security administrator, network administrator, or auditor, you will learn how to make the process easier and demonstrably complete. A few technical terms are included in the Appendix, but you don't need to read them to manage well.

This will take some up-front effort, but will:

- Reduce future effort needed
- Avoid future disruption to operations
- Give you information you need to manage
- Give you tools to demonstrate compliance.

Background

Imagine that, as CIO, you learn that there has been a change, either in the accepted technology for encryption or in the regulations. (You remember when the DES algorithm was replaced with AES. You remember too when new regulations like GDPR, HIPAA, and SOX came down.)

You know the auditors are coming next month to evaluate how well your shop complies with encryption requirements. Here's what you will want to have in place before that happens, starting with some well-known management principles:

Basic Principles of Managing Anything

We start with basic steps. You can't manage anything if you don't:

- Have someone responsible for implementing it
- Know what it includes, how big it is, that is, an inventory
- Have a clear understanding of the requirements
- Have an easy way to compare what you have to what is required

What You Want to Do

First, make someone on your staff responsible for managing all encryption activities on all platforms in your installation (including UNIX, Windows, mainframes, the cloud, your internal networks, and the Internet). As the management consulting expert Peter Drucker said, "If it isn't someone's job, then it won't get done." Put this in writing in a formal policy. Make it the responsibility of someone good on your staff. Give her the authority to make it happen.

Second, issue a standard to all staff stating briefly who your Encryption Manager is, and requiring each application manager to inform the Manager of the names of all their applications, specifying which use encryption, what encryption they use, how, and why. Application managers should consult with application owners to collect opinions about what data needs to be encrypted.

Your Encryption Manager should be able to develop a complete list, or inventory, of all your applications on all platforms. This list should specify which use encryption and which don't, as specified by the application managers. For those with encryption, the list should include what encryption is used, as well as the how and the why, based on the application owner's evaluation of what data is sensitive. (If you already maintain an inventory of applications, then the encryption elements can be incorporated into it, eliminating possible duplication of data.)

Third, ask your Encryption Manager to consult with your Legal and/or Compliance departments to identify what regulations apply to each application's data. (It would be unreasonable to ask any IT staff member to know what regulations and laws apply. That is why you have Legal and Compliance departments.) At this point you should have an inventory of applications that do and don't use encryption, supported by statements from the application owners and the legal experts of why the encryption is needed.

Fourth, ask your Encryption Manager to identify any applications which are not adequately using encryption, including applications which don't use encryption, even though they should. Request that the appropriate managers on your staff fill any gaps. Ask your Encryption Manager for periodic updates. Request your Encryption Manager to document the procedures used to maintain encryption details in your inventory of applications.

In Summary, you now have the management tools in place to respond quickly and easily to any change in encryption technology or regulations. You can demonstrate to the auditors that you have determined encryption requirements from the experts (application owner and legal staff). And you are meeting those requirements.

This takes some initial work by your staff. But it leverages each manager's knowledge and authority to minimize the work each has to perform. Once the procedures are in place, ongoing maintenance should be a reasonable amount of effort. (Beyond what we describe here, you will want to know that the technicians responsible for actually implementing encryption on each platform have done so effectively. But that is a completely separate task, to be addressed in a separate white paper.)

Best of all, you'll have more reason to feel comfortable that you are providing the security your organization needs to protect its data.

A note on what to expect from auditors: Auditors more and more are asking for what they call **TOD** or Test of Design documents. This means formal description of the management controls (policies, procedures, and standards) that you put in place to achieve adequate security. What we describe above will meet those requirements.

If you don't provide a standard against which to audit you, auditors are likely to use either their opinions or commonly accepted standards, such as the STIGs, FIPS, and government Special Publications. These are described in the following appendix.

Appendix: Vocabulary And Buzzwords to Know

Cleartext is the version of a message before it is encrypted or after it gets decrypted.

A **key** is the number used to encrypt or decrypt. The key and the cleartext are the input to the encryption process. The encrypted message and (perhaps a different) key are the inputs to the decryption process. In general, the longer the key, the harder it is for someone to guess it, or to learn it by brute force.

Symmetric Encryption is encryption using an algorithm with which the same key is used to decrypt as to encrypt.

Asymmetric Encryption is encryption where a different key is used to decrypt from the one used to encrypt. The keys come in pairs (one secret and one public) which are linked mathematically. Symmetric encryption is used when you control both ends of a conversation. Asymmetric encryption is used over a network when you control only one end of a conversation. An example would be when you want to accept credit cards on your computer (which you control) from someone somewhere in the Internet (which you don't control). Asymmetric encryption relies on digital certificates.

A **Digital Certificate** is a message which tells you someone's public key (of the public key / private key pair used in asymmetric encryption).

Data-In-Flight is data transmitted over the network, including your internal network and also the Internet.

Data-At-Rest is data stored on tape or disk or in memory or other fixed location.

Enterprise-Wide Encryption is encryption covering all computers and networks in an organization. Most organizations now have their Windows servers, UNIX servers, and mainframes connected in a single internal network, which is also connected to the Internet. For this reason, it makes sense to address encryption comprehensively rather than a computer at a time.

DES (Data Encryption Standard) is an algorithm or mathematical formula used for symmetric encryption. It is now considered obsolete, having been replaced by AES.

AES (Advanced Encryption Standard) is an algorithm used for symmetric encryption. It is the currently accepted, most commonly used symmetric algorithm.

SSL (Secure Sockets Layer**)** is an algorithm used for asymmetric encryption. It is now considered obsolete, having been replaced by TLS.

TLS (Transport Layer Security) is an algorithm used for asymmetric encryption. It is now the currently accepted, most commonly used asymmetric algorithm.

VPN (Virtual Private Network) is the establishment of an "encrypted tunnel" on a public network, allowing you to send and receive data securely without it being read by others on the public network.

HIPAA (Health Insurance Portability and Accountability Act) is a Federal government regulation specifying that you are responsible for protecting sensitive medical data in your care.

GDPR (General Data Protection Regulation) is a regulation of the European Union which may apply to data in your care, even if you don't operate in the EU.

SOX (Sarbanes-Oxley) is a Federal government regulation specifying that executives will be held accountable if they do not adequately protect data in their care.

STIGs (Security Technical Information Guides) are Federal government standards specifying recommend security settings for various types of computers and the software running on them. For example, there are STIGs for Windows computers, iPhones,

UNIX computers, mainframes, and many more. You can download free versions of the STIGs by Googling for example “STIG Windows”.

FIPS (Federal Information Processing Standard) is a set of written standards for information processing from the Federal government. For example FIPS 140-2 provides standards for cryptologic modules. Addendum A to FIPS 140-2 states which encryption algorithms are considered standard. Many organizations have committed to compliance with FIPS 140-2. You can download a free pdf of these documents Googling for example “FIPS 140-2”.

SP (Special Publications) are published by the Federal government to provide useful information for various functions, including security. For example, SP 800-53 is titled “*Security and Privacy Controls for Federal Information Systems and Organizations***”.** You can download free pdfs of these by Googling for example “SP 800-53”.

About the Author: Stu Henderson is an experienced system programmer, auditor, trainer, and consultant, specializing in information security. He is editor of the ***RACF User News*** and the online ***Mainframe Audit News***. He teaches seminars nationwide, both public sessions and in-house, as well as online. His website www.stuhenderson.com contains a wealth of articles and useful links.

