Encryption Policies: A Task-Oriented Approach

Robert Elmore

January 31, 2001

Summary

This paper presents a comprehensive set of encryption policies and best practices that should be considered by an organization. Encryption policies should present what encryption requirements apply in a particular situation, and provide guidance to the user on how to make decisions regarding encryption solutions. Policies should allow salient issues to be brought quickly to the user's attention, and clearly state what is required for policy compliance. It is important to avoid redundancy in the policy document by ensuring that encryption-related topics are grouped together.

This paper structures encryption policies using a practical, task-oriented approach. A task-oriented approach to creating encryption policies seeks to provide guidance on when encryption is required and how encryption should be implemented, based on common business activities. Two areas of business activities require policies on encryption:

1. Encryption policies must address activities that store or transmit sensitive information to ensure that the information remains confidential.
2. Encryption policies must address the general issues of selecting and implementing an encryption process, as well as handling encryption key management.

After presenting ten encryption policies (and corresponding best practices), this paper outlines potential impacts to an organization's environment. If these encryption policies were followed, an organization would need to examine business practices for protecting sensitive information on laptops, servers, and back-up storage media. Sensitive e-mails, remote administration for system administrators, and transmission of sensitive information across unsecured networks are other areas that require review. An organization should also explore how to handle message recovery issues, Federal regulations, organizational structure, and the usefulness of an internal PKI system.

Encryption Basics

Encryption is the process of making information unreadable by unauthorized persons, and is used to protect the confidentiality of information [1,2]. There are three parts to the encryption process:

1. Message. This is the information that the user wants to store or send, and keep confidential.
2. Encryption algorithm. This is a mathematical process that transforms the message from clear text into unreadable cipher text. It is not necessary to keep the programs that perform this processing secret. In fact, it is preferable to use encryption algorithms that are open-source, and have been thoroughly reviewed and tested by the cryptographic community.
3. Encryption key. The encryption key or encryption key pair is used by the encryption algorithm to encrypt and then decrypt the message. Except for the public half of a public/private key pair, it is crucial that the encryption key be kept secret.

There are two major types of encryption processing.

1. Symmetric encryption (also known as private key encryption). This encryption process uses the same secret key to both encrypt and decrypt a message. It requires that the secret encryption key must be previously shared between the sender of the message and the recipient. Examples are the DES and Triple DES algorithms.
2. Asymmetric encryption (also known as public key encryption). This encryption process uses a public/private key pair, where the public key is available to anyone and the private key is kept secret. The sender uses the public key of the recipient to encrypt the message, and the recipient uses the corresponding private key to decrypt. An example is the RSA algorithm.

Encryption adds value for an organization in protecting confidentiality of sensitive information in two major areas:

1. When the organization loses the ability to physically control information, so that information is at risk of being read or stolen. Examples are when information is taken outside of a secure computing environment, taken off the organization's premises, or transmitted across a communications network.
2. When there is the possibility that an employee might risk his or her career, and risk potential criminal prosecution, in order to read, copy, or alter information without authorization. Most likely, the employee perceives that there are personal financial benefits that outweigh the risks.

   In addition to considering encryption as a solution to mitigate this personnel threat, it is important to conduct adequate background checks of employees with access to sensitive information. It is also important to ensure an appropriate level of monitoring and ongoing review is conducted.

Activities Requiring Encryption

Encryption policies should provide guidance on when encryption is required for specific business activities. The policies should also provide guidance on how to select and implement encryption systems to support business processes.

Activities that store or transmit sensitive information may require encryption to ensure that the information remains confidential. These activities might be part of a mainframe or client/server application that supports a business area. Or an individual user might need to protect e-mail and individual personal files at the desktop. Encryption policies should address requirements in the following areas:

1. When is encryption required for storing information on electronic storage media?
2. When is encryption required for transmitting information across a communications network?
3. What encryption practices are required when an individual user wants to protect work files, e-mail, and personal information?

Some information must be classified as sensitive due to Federal regulations, such as Privacy Act [3] information. Other information needs to be assessed for the risks and consequences of disclosure (i.e. loss of public trust, compromised proprietary information, potential for fraud, or manipulation for financial gain) in order to determine whether it is sensitive.

If encryption processes are not implemented and configured properly, they can cause system performance degradation or operational hurdles for the user. In addition, improperly configured encryption processes can give an organization a false sense of security; thinking that the confidentiality of sensitive information is protected through encryption, when in fact it is not. Policies must address the general issues of selecting and implementing an encryption process, as well as handling encryption key management. Policies must also assign accountability for creating encryption standards for specific encryption processes. The following areas should be addressed:

1. What are the requirements when purchasing encryption technology or developing an application that uses encryption features?
2. What are the requirements when implementing and managing an encryption process?

Common Pitfalls When Developing Encryption Policies

Two common pitfalls are often encountered when developing encryption policies:

1. Encryption policies might cover all the important encryption issues, but because they are often spread throughout the policy document, it is difficult to get a complete picture of encryption compliance requirements.

    a. It is difficult to know exactly what activities require encryption because there is no single place the user can turn to and get the complete picture.
    b. The policies do not present a clear integration of encryption policies as they relate to different activities. For example, the policies may present encryption requirements in areas such as information classification, choice of technology (i.e. VPN), and administrative activity (i.e. remote administration of firewalls), but the user must determine how to integrate them together.

1. Encryption policies do not distinguish between the different types of encryption technologies for protecting the confidentiality of information (for example, between public key encryption and symmetric key encryption). The user is left to figure out whether an encryption policy applies to a particular encryption implementation, which can open the door for misinterpretation.

    Using phrases like "all encryption keys" are misleading because a policy usually applies to only one type of encryption technology, and is not applicable to "all" encryption types.

Task-oriented Encryption Policies

In general, information security policies must be written in clear, easy-to-understand business language [4,5] that incorporates the following points:

1. Information Security policies should be brief and to-the-point.
2. Information Security policies should address a real risk or protect something of value to a organization.
3. Information Security policies should relate to a commonly performed task.
4. Information Security policies should reflect requirements to which an organization’s staff must comply.

Task-oriented encryption policies directly relate to real activities and real issues in an organization’s environment that require encryption processes or support encryption services. For each business activity, it is important to provide a brief description of the activity, define what encryption policies apply and why, and present general comments to further explain the scope and implication of the policy.

Encryption policies are intended to protect sensitive information, based on an organization’s information classification scheme. It is important to acknowledge that the business owner of the information resource is ultimately responsible for determining what information should be classified as sensitive and assessing the risks to the information if a breach of confidentiality were to occur. However, encryption should not be limited to protecting only sensitive information resources. If appropriate, these encryption policies can also apply to other information classifications, such as for critical resources or for internal use only resources.

All areas must comply with encryption policies; otherwise, an exception to the policy should be filed (and approved prior to implementation) if the policy requirement is not met.

As appropriate, a recommended best practice should be included with an encryption policy. Best practices present the preferred method to provide protection for sensitive information. The choice for following the recommended best practice depends on analyzing business needs, risks, application functionality, and required user features.

Benefits of Task-oriented Policies

The desired benefits of structuring encryption policies along a task-oriented approach are:

1. To have users easily understand what must be done to comply with encryption policies, to have users understand the reasons for the policies and why compliance is important, and to provide flexibility to users when identifying what sensitive business information requires encryption.
2. To have users consult encryption policies early on when working on a task or project, avoiding the scenario where users wait to consult policies until it is so late in a project's timeline that exceptions must be generated because there is not enough time to comply.
3. To provide clear easy-to-understand encryption policies in order to minimize unnecessary phone calls to a central policy group, who must take the time to explain policy requirements.
4. To provide value-added guidance for real business issues, so that users are encouraged and motivated to comply with encryption policies because it makes business sense to do so.
5. To avoid encryption policies that are difficult for the user to adopt, so that the policies are simply ignored. In other words, encryption policies should not build hurdles for the user. Once users begin to ignore information security policies, there is a tendency to just continue ignoring policies in subsequent projects and situations.

Guidance on When Encryption is Required [6,7]

Users have a need to protect the confidentiality of sensitive information, and should turn to information security policies for guidance on when it is necessary to use encryption to provide that protection. Sensitive information must be protected against unauthorized disclosure when it is stored on electronic storage media and when it is transmitted across a communications network. Individual users, especially executives, need guidance on how to use encryption for protecting sensitive e-mails and desktop files.

When is encryption required for storing information on electronic storage media?

Policy #1: Information must be encrypted when stored on electronic storage media:

- If the information cannot be protected using sufficient physical or logical controls, and the information is at risk of being stolen.
- If the information is considered too sensitive for system administrators or operators to read.

Recommended best practice: For information that is copied and backed-up onto electronic storage media for off-site site storage at a non-organization facility, it is recommended that the entire electronic storage media should be encrypted before sending off-site. Locking the media in sealed cases is a less secure, but acceptable alternative.

Recommended best practice: For traveling users, it is recommended that the entire hard disk on a laptop should be encrypted, due to the difficulty in providing sufficient physical controls to prevent the laptop from being stolen.

Recommended best practice: Encryption keys should not be stored on the same electronic storage media as the information that has been encrypted using the keys. If it is necessary to do so, encryption keys should be restricted using an access control mechanism to only authorized users and authorized processes. The use of hidden files or hidden directories is not an acceptable alternative.

General Comments: An organization's information is often processed and stored in a physically secure computing environment. For example, the mainframe environment is considered a secure computing environment, and support staffs such as systems administrators or system operators have the responsibility to ensure the ongoing successful processing of applications. Access control mechanisms govern what information can be accessed and at what level. Access to information, including information classified as sensitive, is most likely protected in a secure computing environment. However, system administrators and system operators often have privileged access to all information. An additional layer of protection, on top of the access control system, is required for information that is too sensitive for even system administrators or operators to read. Encryption is a solution for providing this additional layer of protection.

Information processed and stored in a distributed computing environment, for example on an application server or web server, may not be as secure as the traditional mainframe environment. To achieve a secure computing environment for servers, it will be necessary to place servers in a physically secured location, harden the servers by removing all unnecessary services, and create a secure perimeter with firewall protection.

Once this scenario is in place for the server environment, the same decision regarding encryption can be made. System administrators often have privileges that allow access to all information on the server. If the information processed by and stored on a server is too sensitive for server administrators to read, then encryption is required to provide the necessary protection for sensitive files. If the server environment cannot be considered a secure computing environment, then a broader application of encryption (such as encrypting the entire server hard disk) might be necessary to protect the information.

Following are examples of sensitive information that require additional protection:

- Information with regulatory requirements, such as specified in the Privacy Act [3].
- Information such as Human Resources data on payroll, disciplinary actions, or employee medical records.
- Passwords and passphrases.
- PINs.
- Symmetric encryption keys.
- Individual user private encryption keys and digital certificates.
- Private encryption keys and digital certificates assigned to system components.

As long as information remains inside the physically secure computing environment, there is minimal risk of it being stolen. Once information stored on an electronic storage media leaves the secure computing environment, it is at significant risk for being stolen, and encryption provides a solution to ensure the confidentiality of information were a breach to occur. Even if the information is stolen, it cannot be read by the thief without the associated encryption key.

While other alternatives exist, encryption is considered the best solution for ensuring confidentiality of information if there is risk of a loss of physical control. Following are examples where encryption would be useful when electronic storage media is taken off-site from an organization's premises:

- Laptop hard disk for a traveling executive or employee. Recent news stories have reported that laptops are at great risk of being stolen from airports, hotels, meeting rooms, and other public places.
- Laptop or desktop workstation hard disk for an employee who works from home (i.e. telecommuter). This might be important since the organization cannot prevent the telecommuter from installing a DSL line or cable modem, or ensuring that a personal firewall is always active.
- Back-up media (tapes, diskettes, CDs) that are sent to an off-site storage facility. Back-up media are often handled by third-party services that are not under direct control of an organization. This area can easily be compromised; due to low skill-levels of people hired by the third-party or poorly implemented physical controls by the third-party over handling the back-up media.

When is encryption required for transmitting information across a communications network?

Policy #2: Information must be encrypted before transmitting over a communications network:

- When using an external public communications network, the information is considered too sensitive for the general public to read.
- When using an external public communications network, the information must be protected to comply with Federal regulations on consumer privacy.
- When using the internal communications network, the information is considered too sensitive for a general computer user to read.

Recommended best practice: It is recommended that remote administration of hardware, software, or applications should be performed over an encrypted communications session.

General Comments: In today's world, interconnectedness is a given, and sharing information is a fundamental fact of doing business. Organizations will utilize a combination of communication networks to connect internal secure computing environments (or secure enclaves) with each other, connect the organization with its business partners, and connect the organization to the outside world through the Internet. All of these areas have a need to share information with each other across communication networks.

Once information has left a secure environment, the packets of information cannot be physically controlled as they travel across a communications network. The communications network could be either the internal network or the Internet. And with the loss of physical control comes the increased risk of theft, or of being intercepted. Once intercepted, information can be read, altered, or redirected by an unauthorized person. If the transmitted information is sensitive enough so that a general user should not be able to read it, then encryption is required to protect the confidentiality of the information.

Following are examples of sensitive information that require encryption protection when transmitted across a communications network:

- E-commerce transactions that contain private customer information.
- Information such as Human Resources data, or sensitive data used in other business areas.
- Audit trails or logs.
- Logs from intrusion detection systems.
- Security event data.
- Passwords, passphrases, and PINs.
- Symmetric encryption keys, private encryption keys, and digital certificates.

A special situation occurs when an employee performs system administrative tasks remotely over a communications network, for example performing problem-resolution or maintenance to a server or firewall. If the system administrator has powerful privileges on the system component so that a compromised remote session by an attacker would have serious consequences, then encryption of the remote administration session is a recommended best practice. Solutions such as a virtual private network (VPN) or Secure Shell (SSH) should be considered.

What encryption practices are required when an individual user wants to protect desktop work files, e-mail, and personal information?

> Policy #3: An individual user must only use encryption products and processes approved by a central systems security group for the following business activities:
>
> - Encrypting a saved e-mail.
> - Sending an encrypted e-mail.
> - Encrypting a desktop work file.
> - Protecting a personal private key or digital certificate
>
> Other Related Encryption Policies
>
> Refer to Policy #4 for requirements that establish accountability for approving encryption products and processes.
>
> Refer to Policy #5 for requirements on message recovery and comments on acceptable key escrow methods.

General Comments: Providing an encryption service to individuals is a very important area, especially encryption services for executives and traveling users. It is crucial that individuals have the ability to encrypt sensitive e-mail messages and desktop work files. It is equally important that the organization has some means of message recovery, i.e. the ability to decrypt an individual user's encrypted e-mail or desktop work file if the individual is not available due to illness, resignation, or termination.

There are two important areas that must be considered when selecting the encryption methodology.

- Speed and ease-of-use. Encryption of e-mail messages or desktop work files must not take a long time to process and must be easy for the individual user to accomplish. If not, users will either avoid encrypting information that should be kept confidential, or will circumvent the policy and implement their own encryption scheme.
- Consistent, or at least interoperable, technologies. If the organization wants the ability to easily administer e-mail encryption and a message recovery process, then it is necessary that users not be allowed to implement their own encryption schemes, because an inconsistent approach would quickly become unmanageable and difficult to administer. In addition, if users created their own public/private key pairs, they would have to share the public key with users prior to sending an encrypted message. In an environment with several thousand users, this approach would quickly get out-of-hand.

  > Requiring a central group within the organization to select a single encryption method (or perhaps several interoperable methods) for individual users adds significant value to the organization and supports productivity that is more efficient.

When selecting an encryption solution for e-mail and desktop files, flexibility is an important consideration. In some cases, the user will need to have the ability to select whether or not encryption is necessary to ensure confidentiality of information. Examples of the types of information where the individual user selects encryption are:

- Desktop work files, spreadsheets, and documents.
- Stored or saved personal e-mail messages.

In other cases, the user must be required to protect some types of information using the organization's standards. Examples are:

- Private encryption key.
- Digital certificate.

Encryption solutions for the individual user range from a stand-alone software package that interfaces with an e-mail application on each desktop (such as PGP) to a full-scale PKI system that integrates with a variety of mail servers. The best implementation will most likely be a set of products and tools to provide encryption services to the individual user depending on the user's role in the organization and business needs for handling confidential information. Whatever the solution, it must be easy for the user to use, relatively fast, and as transparent as possible. Otherwise, the solution will not be accepted.

Guidance on How to Select and Implement Encryption **[6]**

The following encryption policies are primarily intended for information technology departments. The policies address what is required when building an encryption process for other business areas to use. Encryption policies are applicable for the following activities:

- Purchasing and implementing an encryption product.
- Purchasing and implementing commercial off-the-shelf (COTS) software that has encryption features.
- Developing an application with encryption features.

What are the requirements when purchasing encryption technology or developing an application that uses encryption features?

> Policy #4: All encryption products and processes must be approved by a central systems security group, and configured according to standards set by the central systems security group, prior to use.
>
> The central systems security group must maintain a list of approved encryption algorithms and acceptable key lengths for each algorithm.
>
> Recommended best practice: When selecting an encryption product, it is recommended to purchase a product that is compliant with FIPS-140 [8] standards, or comparable Federal information processing standards.
>
> Recommended best practice: Tamper-resistant hardware encryption products should be selected to provide encryption services before selecting software encryption, if a hardware encryption product is available and if the product meets business specifications.
>
> Recommended best practice: An encryption product specializing in encryption services should be used to protect sensitive information, such as application files and security logs, before relying on commercial off-the-shelf (COTS) software with encryption features, if an encryption product is available and if the product meets business specifications.

General Comments: A central systems security group within the organization that approves and sets standards for encryption products and processes is the best way to ensure that encryption will be used effectively in the organization. Encryption processes can be complex and are often difficult to properly implement. It is important to keep the number of encryption solutions to a minimum (i.e. keep it as simple as possible) and ensure that the selected set of products complement each other.

Standards established by an organization can provide assurance that encryption products selected for the organization's environment use technologies that have been proven to be secure over time, because the products have been adopted by a national or international standards group and have been tested using open-standards procedures by the cryptographic community. Encryption products should be implemented using a minimum encryption key length to ensure sufficient protection.

If the organization is a Federal agency, it may be required by law to purchase products that comply with FIPS-140 [8] requirements. It is a recommended best practice that a FIPS-140 compliant encryption product be selected, if one is available and if it meets business specifications. Government regulations might require the use of FIPS-140 compliant encryption products even in domains where it is not necessary.

Encryption services managed by an encryption hardware device are more secure than encryption services implemented in software. Encryption hardware makes it possible for encryption keys never to be displayed in clear text. If tampering is detected, the encryption hardware device can be set to zeroize memory making the hardware device unusable. Encryption services implemented in software must constantly ensure that the encryption key is secured and protected from unauthorized access. It is a recommended best practice that tamper-resistant encryption hardware be selected if it is available and if it meets business specifications.

It is also a recommended best practice that a product specializing in encryption be used instead of relying on a commercial-off-the-shelf (COTS) product that has encryption services. COTS software often uses a proprietary encryption algorithm, rather than an open-standard encryption algorithm that has been thoroughly reviewed and tested by the cryptographic community. Use of a proprietary encryption algorithm that has not been reviewed and tested by the open-standards process is generally thought to be a weaker implementation of encryption services.

Policy #5: Encryption products or processes must provide message recovery capabilities.

The central system security group must maintain a list of the types of encrypted information that are excluded from message recovery or key escrow requirements, such as encrypted password files and digital signatures.

General Comments: A solution for providing message recovery is to implement a key escrow process. Symmetric encryption keys and private keys used for encryption should be escrowed in one of the following ways:

- The encryption key is manually escrowed with management.
- The encryption key is manually escrowed with the central systems security group.
- The encryption key is automatically escrowed as part of the native operation of the encryption system or application software. The system supports either key escrow or administrative data recovery.

Private keys used for digital signatures should not be escrowed and should be excluded from any key escrow requirements.

Depending on the sensitivity of the information that is encrypted, escrowed encryption keys that are stored manually may need to be stored using principles of dual control.

What are the requirements when implementing or managing an encryption process?

Policy #6: Any symmetric or private encryption key that is compromised must be immediately changed and a new encryption key generated.

Policy #7: Secrecy of a symmetric or private encryption key must be maintained until all the information protected by the key is no longer considered sensitive, and is declassified by the business owner.

Policy #8: For master/root encryption key(s) that are entered manually to initialize an encryption system, the following controls are required when handling cleartext encryption keys:

- Encryption key(s) must be split into separate key parts.
- Encryption key parts must be handled using principles of dual control and separation of duties.
- Encryption key parts must be stored using some means of physical security.

Recommended best practice: An independent party, such as an auditor, should be present when master/root encryption key(s) are loaded as part of the initialization of an encryption system.

Policy #9: For symmetric encryption key(s) that are distributed manually to facilitate subsequent transmissions of an encrypted message, the following controls are required when handling cleartext encryption keys:

- Encryption key(s) must be split into separate key parts.
- Manual distribution and input of encryption key parts must be handled using principles of dual control.
- Encryption key parts must be distributed over a communication channel that is different than the channel used for transmitting information protected under the encryption key.
- Encryption key parts must not be shared without written authorization from management.
- Encryption key(s) must have a stated life and be must be changed on or before that date.

Policy #10: For asymmetric public/private key pairs:

- When generating public/private key pairs for individual users, distinct sets of public/private key pairs must be generated for different business functions; for example: one set for encryption activities and another set for signing transactions with a digital signature.
- When generating public/private key pairs for system components, separate sets of public/private key pairs must be generated for different business activities: one set for each of the separate business functions performed by the system component that require encryption or digital signature services.

Recommended best practice: It is recommended that private keys for individual users should be stored securely either in an encrypted file on the user's workstation or using smart card technology. Private keys for system components should be stored in a hardware encryption device.

General Comments: These encryption policies provide specific requirements for handling different types of encryption keys. The policies present 'what' is required, and procedures will need to be created by the organization's staff to document details on 'how' the policy requirements will be executed.

The requirements contained in these encryption policies try to address a concern with typical encryption policies, where no distinction is made between the different types of encryption keys. It is often difficult to know which policy requirements to follow because a single policy does not apply to all types of encryption keys, and the reader is left to determine whether the policy applies.

These encryption policies distinguish between three different encryption key types:

- Master/root encryption keys.

  These encryption keys are at the top of the encryption key hierarchy for a particular encryption system. They are manually loaded to initialize an encryption system, and usually the encryption key values do not change because that would potentially mean changing all keys generated under the master/root key. This is why dual control, segregation of duties, physical controls, and presence of an auditor are important policy requirements.

- Symmetric encryption keys.

  In this encryption scheme, the same encryption key is used to both encrypt and decrypt the message. Symmetric encryption keys are usually used to encrypt a large bulk of information. Due to the difficulty in keeping the keys secret, they should be changed periodically. When software encryption is used, symmetric keys often must be distributed manually, which presents a challenging key management issue. When hardware encryption is used, key management for distributing the symmetric keys is usually handled by the hardware device, which allows the key to be changed automatically, often with each communications session.

- Asymmetric public/private key pairs.

  Asymmetric key pairs usually do not change, unless the private key is compromised. They are primarily used for three functions, (1) to encrypt the exchange of a one-time symmetric session key, (2) to provide message integrity (through creation of a message digest by the sender that can be compared when the message is received by the recipient), and (3) to provide for authentication and non-repudiation (through the use of a digital signature for an individual user). Public/private key pairs also facilitate the implementation of a process for encrypting e-mails.

Following are the important areas of encryption key management, and must be considered when implementing an encryption process. It is necessary to develop specific procedures for each of these areas.

- Generation
  - Ensure the encryption product generates encryption keys using strong random number generation techniques and selects the random number from the full range of possible values.
  - Ensure keys cannot be leaked (or copied) when they are generated.
- Distribution
  - Ensure encryption keys get to the recipient at the point of intended use. If encryption keys are manually distributed, it is necessary to follow secure key exchange requirements.
- Implementation
  - Ensure encryption keys are properly installed into the encryption software or hardware device where they are going to be used. If encryption keys are manually entered, it is necessary to follow requirements for dual control.
- Storage
  - Ensure encryption keys are stored securely in the software or hardware device. (Software encryption is acceptable, but a tamper-resistant encryption hardware device is better.)
- Changing
  - Master/root encryption keys are usually never changed.
  - Symmetric encryption keys must be changed periodically.
  - Asymmetric public/private key pairs must be changed if the private key is compromised.
- Control
  - Ensure encryption keys are used for their intended function. For example, a private key for signing messages should not be used to encrypt data.
- Disposal
  - Ensure encryption keys are properly disposed of. This is less of a concern when encryption keys are changed automatically.

Impacts to an Organization’s Environment

Following are the areas of encryption practices that have potential impact to most organizations:

- Laptop hard disk encryption.

  If a laptop is at risk for being stolen, then the laptop’s hard disk should be encrypted. This encryption practice should be required for all laptops in the organization, unless there is some way to physically secure the laptop. A stand-alone encryption product that integrates with the laptop should be selected, perhaps in conjunction with biometric authentication.

- Server encryption.

  Encrypting files on a server has security limits if the encryption key is stored in software on the same server. This approach does little to minimize the threat of a remote attacker (external or internal), because the encryption key is vulnerable once the attacker has compromised the server. A better approach would be to use a tamper-resistant hardware encryption device for encrypting selective files on the server or the server hard disk, if the business application warrants it.

  For web servers, an organization should ensure that all SSL private keys are properly protected using some method of server file encryption.

- Encryption for back-up storage media.

  Back-up electronic storage media (tape, diskette, or CD) that is given to a third-party for off-site storage is at risk for being stolen or used in an unauthorized manner. Third-party vendors that provide off-site storage often employ staff who are less inclined to follow security procedures, and can lose back-up media or give the media to an unauthorized person, either intentionally or in error. Encryption provides a strong solution for ensuring that the electronic storage media, even if were to be misplaced or stolen, could not be read by an unauthorized person.

  An alternate solution is to lock storage media in a tamper-detective box. This approach, while certainly a deterrent, can only detect a breach of confidentiality and cannot prevent it from occurring.

- E-mail encryption.

  An e-mail encryption solution is an important area for an organization to implement, and it requires careful planning. It is an area that needs to be gotten right; otherwise users will be frustrated if the solution is not relatively fast and easy-to-use. Careful planning is also required so ongoing administrative support does not turn into a complex, unmanageable process.

  Given a large number of e-mail users, an encryption solution that must be individually customized for each desktop is not recommended. It is preferable that the central e-mail system provide either its own solution for sending or storing encrypted e-mails (by generating digital certificates for users defined to the e-mail system), or hooks into a PKI solution (where digital certificates generated by the PKI can easily be imported into the e-mail system).

- Session encryption for remote administration of system components.

  System and network administrators usually have privileged accounts on an organization’s system components. When an administrator connects remotely to a system using a privileged account, there is a significant risk that a compromised session would give an attacker powerful access to the system component.

  Remote administration sessions must be encrypted. Examples of possible technologies are Secure Shell (SSH) or a Virtual Private Network (VPN).

- Encryption for transmission of information between secure computing environments.

  The organization's internal network may be supported by a third party vendor. The organization must assess whether the eavesdropping threat of a general user or someone from the third-party vendor listening in on internal transmissions is great enough to warrant encryption of transmissions between secure computing environments. If so, then enabling encryption on routers or network devices, or installing separate link encryption devices are possible solutions.

  This layer of network encryption would be in additional to any e-mail or file encryption used to protect sensitive information as it is transmitted from one secure computing environment to another.

- Message recovery issues.

  At some point, the organization will need a message recovery program to ensure sensitive encrypted messages that are critical to the ongoing operations of the business can be recovered. This will be important if the individual who encrypted the message is unavailable either due to illness, vacation, resignation, termination, or death. There also may be legal issues for ensuring message recovery, especially in areas of the organization that are responsible for contracts, purchases, and labor negotiations.

  This is another area that requires careful attention and planning, and a formal key escrow program is one solution to achieve message recovery. There will probably be several different ways needed for escrowing encryption keys, and it will be crucial to document all of the methods to ensure no areas are overlooked.

  An internal PKI might be helpful in this area, if the selected product automatically handles the key escrow process.

- FIPS-140 compliance.

  Federal Information Processing Standards Publication (FIPS) 140-2 [8], "*Security Requirements for Cryptographic Modules*," is the standard that is accepted in the United States as a method of measuring the security assurance of cryptographic products. The National Institute of Standards and Technology (NIST) and the Canadian Communication Security Establishment (CSE) developed the standard. Independent third-party labs test cryptographic products against FIPS-140-2 criteria to validate the level of security assurance provided by the product.

  The standard applies to all Federal agencies that use cryptographic-based security systems to protect unclassified information. If the organization is a Federal agency or performs work for a Federal agency, it may be required by law to use FIPS compliant encryption products.

- Crucial role for the central systems security group.

  The success of implementing encryption practices depends on the crucial role performed by a central systems security group. It is important that a central group be responsible for approving encryption products, and setting standards for use. This is especially critical for standards such as the minimum length of encryption keys.

- Internal Public Key Infrastructure (PKI).

  Encryption policies should not drive the decision for an internal Public Key Infrastructure (PKI). However, the existence of a PKI system would add much value in the implementation of encryption schemes.

  An internal PKI system could help with generating public/private key pairs for e-mail encryption. A PKI system could have the capability of escrowing private keys in order to facilitate message recovery procedures. A PKI system could facilitate generating digital certificates for system components that would provide additional options for transmitting sensitive information between secure enclaves. The use of digital certificates for system components mitigates the threat of server spoofing from internal or external attack, and provides the ability to ensure the integrity of transmissions for business transactions, audit trails, or event logs.

  Implementing an internal PKI system requires a significant commitment in terms of both resources and finances. Careful planning is essential to establishing a PKI system.

Conclusion

Encryption policies that are task-oriented help identify and determine those encryption practices that should be considered for an organization’s environment. This paper has presented a set of encryption policies that are task-based, structured in a way to make them as clear as possible to the user, and intended to add value to business activities in order to encourage compliance with the policies.

List of references

[1] Schneier, Bruce. (1996). *Applied Cryptography.* New York: John Wiley & Sons.

[2] Denning, Dorothy. (1999). "Cryptography and Escrowed Encryption." In Tipton, Hal and Krause, Micki, (Eds.) *Handbook of Information Security Management, Volume III*. Boca Raton: Auerbach. http://secinf.net/info/misc/handbook/631-637.html

[3] United States Department of Justice. (1974). "Privacy Act of 1974, as amended." 5 U.S.C. §552A. http://www.usdoj.gov/04foia/privstat.htm

[4] Lindley, Patrick. (2001). "Technical Writing for IT Security Policies in Five Easy Steps." SANS Institute. http://rr.sans.org/policy/tech_writing.php

[5] Flynn, Nancy. (2001). *The ePolicy Handbook: Designing and Implementing Effective E-Mail, Internet, and Software Policies.* New York: American Management Association.

[6] Wood, Charles Cresson. (1999). *Information Security Policies Made Easy, Version 7.* Baseline Software, Inc.

[7] Overly, Michael. (1999). *e-Policy: How to Develop Computer, E-Mail, and Internet Guidelines to Protect Your Company and Its Assets."* New York: American Management Association.

[8] National Institute of Standards and Technology. (2001). "FIPS PUB 140-2: Security Requirements for Cryptographic Modules." http://csrc.nist.gov/cryptval/140-2.htm

List of additional resources

Center for Democracy and Technology. (2002). "Encryption Home Page." http://www.cdt.org/crypto/

Electronic Privacy Information Center. (2000) "Cryptography and Liberty 2000: An International Survey of Encryption Policy." http://www2.epic.org/reports/crypto2000/

Mactaggart, Murdoch. (2001). "Introduction to Cryptography." IBM: developerWorks: Security Library. http://www.detectiondesintrus.com/Documents/Cryptography/S-crypt01.pdf

National Institute of Standards and Technology. "Internet Security Policy: A Technical Guide - Chapter 5.3 Encryption." http://csrc.nist.gov/isptg/html/ISPTG-Contents.html

Schneier, Bruce. (Monthly). "Crypto-Gram Newsletter." Counterpane Internet Security. http://www.counterpane.com/crypto-gram-0201.html

Schneier, Bruce. (2002). "Security Pitfalls in Cryptography". Counterpane Internet Security. http://www.counterpane.com/pitfalls.html

University College, Australian Defense Force Academy. (2002). "Cryptography and Computer Security – Lectures." http://www.cs.adfa.oz.au/teaching/studinfo/csc/lectures/index.html

to top of page | to Reading Room Home