April 2002

ITL Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

TECHNIQUES FOR SYSTEM AND DATA RECOVERY

Bill Burr, Computer Security Division
Joan S. Hash, Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology

Introduction

A key asset in federal agencies today is the information and data used to implement, sustain, and maintain critical government programs and operations. Current efforts in ensuring that the United States can recover and restore activities which have great impact on the physical and economic health and safety of the American public are dependent upon the ability to quickly reinstate information systems and the data required to run those systems. Effective homeland security is dependent upon an extensive amount of corroboration and data sharing.

It is essential that those managing information technology (IT) security programs ensure that they have put contingencies in place for quick restoration of IT resources. A *Business Impact Analysis (BIA)* should be completed. The BIA identifies and prioritizes systems and data in terms of their criticality to an organization's business processes and mission. As part of this process, mission-critical operations should be identified along with the supporting data and systems. Subsequent to identification of these critical assets, methods for recovery of data and systems due to error or attack must be included in the overall *Business Continuity Plan*. This *ITL Bulletin* focuses on techniques for addressing this important component of contingency planning. The intent is to provide users with a quick reference *primer* on methods for data and system recovery.

Contingencies For Data/ System Availability

- ***Offsite Storage***- Critical data should be backed up and stored at an offsite location. Backup media should be housed in a secure, environmentally controlled facility. Information on data content and structure should be stored with the data as well. Any relevant licensing and vendor information should also be part of the backup materials delivered.
- ***Formalized Policy On Backup***- Organizations need to document and enforce policies on backing up critical IT resources. Requirements for this should be defined in terms of the impact on the organization's mission and operations. The backup cycle defined must consider user and customer requirements. Frequency of backup will depend on infrastructure robustness and redundancy, as well as the level of difficulty for reconstruction. Information security policy should define the general broad requirement, and this must be tailored and defined for individual operations. In cases where the data may be potentially needed for legal or investigative purposes, agencies need to consult with their investigative, general counsel, and records retention organizations prior to finalizing retention policies.
- ***Formalized Testing Program***- For all procedures used to address organizational policy for system and data recovery, it is essential that a test plan be developed and executed at least annually to ensure that recovery is achievable under the prescribed scenarios. Based on the test results, the plan should be modified if required.
- ***System Configuration***- System recovery is faster if hardware, software, and peripherals are standardized throughout an organization. Although this may not always be achievable, compatibility is a big factor for easy recovery.

Continued on page 2

ITL Bulletins are published by the Information Technology Laboratory (ITL) of the National Institute of Standards and Technology (NIST). Each bulletin presents an in-depth discussion of a single topic of significant interest to the information systems community. **Bulletins are issued on an as-needed basis** and are available from ITL Publications, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8901, Gaithersburg, MD 20899-8901, telephone (301) 975-2832. To be placed on a mailing list to receive future bulletins, send your name, organization, and business address to this office. You will be placed on this mailing list only.

Bulletins issued since September 2000

- ***Interoperability-*** To facilitate recovery, backup devices must be compatible with operating systems and applications used in backup and recovery operations.
- ***Selection of Backup Media-*** Decisions made regarding what backup media to use need to consider the amount of data to be backed up, the backup frequency and the required retention, recovery and transport requirements, destruction and restoration procedures, availability, and cost. Common media used include diskettes, tape cartridges, removable media (zip drives), compact disks, network storage devices such as networked disks, or server backups. Internet backup or online backup is a commercial service which allows personal computers to back up data to a remote location over the Internet for a fee. Confidentiality procedures need to be addressed up front prior to invoking any of these methods. In addition, it is important to ensure that the necessary hardware remains available to read backups or have a method in place to convert to newer media if necessary.
- **Types of System Backups:**

  ❒ ***Full***- Captures all files selected for backup. Depending on the volume of data and frequency, full backups can require a large storage capacity and a significant amount of time to record the information. In cases where much of the data does not change from backup to backup, other options may be considered.

ITL Bulletins Via E-Mail

We now offer the option of delivering your ITL Bulletins in ASCII format directly to your e-mail address. To subscribe to this service, send an e-mail message from your business e-mail account to listproc@nist.gov with the message **subscribe itl-bulletin**, and your name, e.g., John Doe. For instructions on using listproc, send a message to listproc@nist.gov with the message **HELP**. To have the bulletin sent to an e-mail address other than the From address, contact the ITL editor at 301-975-2832 or elizabeth.lennon@nist.gov.

  ❒ ***Incremental***- Captures only files created or modified since the last backup. This method is more efficient from a storage media perspective, but may require more time for restoration, depending on when the last full backup was taken prior to initiating a recovery operation.

  ❒ ***Differential-*** Stores files that were created or modified since the last full backup. This method takes less time to complete than a full backup and may require fewer storage units than an incremental approach because only the full backup tape and the last incremental tape would be needed for restoration. One disadvantage is that the differential backups take longer because the amount of data since the last full backup increases daily until the next full backup is run.

- ***Redundant Array of Interactive Devices (RAID)***- RAID technology can provide disk redundancy and fault tolerance for data storage and increase the mean time between failure (MTBF), improving data availability. RAID can be used to mask disk drive and controller failures. It can also increase performance and reliability. With a RAID system, disk drives can be swapped without shutting down the system when a disk drive fails. RAID is not, however, a satisfactory substitute for offsite backups, because it offers no protection against catastrophic events such as fires or floods.

  ❒ ***Disk Replication***- With disk replication, data is written to two different disks (a protected server and a replicating server) so that two valid copies of the data are always available.

Offsite Backup Options

To prevent loss of data from catastrophic events such as fires, floods, and the like, it is vital that backups be maintained in a separate, offsite location, so that the probability of a single event destroying both the operational data files and their backup is small. Decisions on what location an organization should use should be based on completion of a formal risk assessment. NIST Special Publication 800-30, *Risk Management Guide For Information Technology Systems*, provides guidance on this issue and is available for download at http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf. Periodic backups of removable media and their transportation to a secure, remote site can, in many cases, accomplish offsite backup. However, automatic remote backup can also be accomplished by:

- ***Electronic Vaulting-*** Allows backups to be created offsite automatically by the use of an electronic vaulting provider. Media that may be used includes optical disks, magnetic disks, mass storage devices, or automated tape libraries.
- ***Remote Journaling-*** Transmits transaction logs or journals to a remote location. This enables transactions, applications, or database changes since the last backup to be recovered.

For both electronic vaulting and remote journaling, offsite facilities are still required.

- ***Alternate Sites***- Three types of alternate sites may be considered for backup and recovery of a system's capability:

  ❒ *Dedicated* site owned and operated by an agency,

  ❒ *Reciprocal* site with an internal or external entity where a formal agreement has been negotiated, and

  ❒ Commercially leased facility.

  Regardless of which type of alternate site is used, there are five possible scenarios that apply.

  Cold Site- The facility has necessary space and infrastructure support (electric power, telecommunications support, environmental controls), but does not contain IT equipment.

  Warm Site-The facility is partially equipped with some of the necessary IT equipment. It is maintained in an operational status ready to receive the relocated system.

  Hot Site- The facility is equipped with all necessary infrastructure and IT equipment to be immediately and fully functional. A hot site is typically staffed 24 hours a day, 7 days a week.

  Mobile Site- A self-contained transportable unit that is custom-fitted with specific telecommunications and IT equipment necessary to meet defined requirements.

Mirrored Site- A fully redundant facility that has real-time information mirroring and is identical in all technical aspects to the primary site.

Cold sites are the least expensive option, with mirrored sites being the most expensive.

It should be noted that other traditional operational contingencies such as the taking of regular backups by system administrators, associated backup documentation, and the process of securing administrative passwords are not addressed in this bulletin but need to be in place to provide a basic level of recovery capability in addition to incorporating any of the additional techniques emphasized above.

Recovery of Encrypted Data

With an increased use of cryptography governmentwide, there is an increased need to advise agencies regarding recovery techniques for encrypted data. The following section provides information on encryption methods and considerations for effective data recovery.

Key recovery is the generic term for the *systematic protection of encryption* keys to prevent their loss. NIST is developing comprehensive guidance on the full lifecycle of key management, including the generation, use, protection, and destruction of keys. Here we address only one important aspect of that broader subject, key recovery.

Key recovery may be needed for two reasons:

- ❒ *if keys used to encrypt data with strong encryption are lost*, then the data is lost.
- ❒ *lost keys may affect the continuity of operations.*

Encryption is used to protect sensitive information when it is stored in IT systems and when it is transmitted between them. NIST-approved encryption algorithms offer strong confidentiality protection. Data encrypted with NIST-approved strong encryption algorithms can only be decrypted with the key that was used to encrypt the data. On the one hand, to ensure the confidentiality of encrypted data, the encryption key must be carefully protected; however, if the encryption key is lost, the data is lost. *Therefore it is vital that encryption keys*:

- ❒ *be carefully protected from unauthorized access*, but
- ❒ also *be carefully protected from loss,* even if the "owner" of the key leaves or is unable to perform their duties.

The loss of encryption keys may affect the continuity of operations, even if it does not cause data loss. In addition, the loss of authentication keys or signature verification keys may also affect the continuity of operations. These keys may need to be copied (i.e., backed up or archived) in order to allow recovery of the keys, when required. However, in many cases, it is unnecessary and may be undesirable to copy or back up the private signing keys used to create digital signatures. *In general, implementing key recovery for the private signing keys is undesirable, because it weakens "non-repudiation*" since the key holder does not have sole control of their signing key. Because of this disparity in the need to back-up keys, it is usually undesirable to use one key for multiple purposes (e.g., for both encryption and digital signatures).

Users primarily need key recovery for stored encrypted data. Although it may, in some cases, be desirable to implement key recovery for encryption keys used during communications, in most cases the loss of such keys does not cause data loss. This is because encrypted data communications protocols such as the Transport Layer Security (TLS) or Secure Socket Layer (SSL) protocol generally decrypt data immediately when it is received. Encrypted e-mail systems are an exception, since, in many products, encrypted messages may be saved in encrypted form.

Key recovery generally requires that a copy of all the keying material needed to recover data or resume operations be securely maintained in the custody of a trusted key recovery facility or officer which is not the normal owner or user of the encrypted data or keying material. Any keying material maintained for key recovery is an additional point of attack, and therefore, the security of data maintained for key recovery purposes is paramount. In many cases, it is desirable to maintain the key to be recovered under dual control, so that the cooperation of two or more people is required to recover a key.

There are a large variety of encryption mechanisms and products, and it is impossible to summarize here how they all maintain and manage their keying material. *The keying materials that require backup and secure storage for key recovery purposes may include*:

- ❒ keys used to decrypt data;
- ❒ keys used to decrypt encryption keys that are used to decrypt data;
- ❒ keys used to authenticate data;
- ❒ keys used to verify digital signatures, and
- ❒ (in unusual circumstances, where operationally required) private signing keys.

In addition, some other information may need to be available in order to recover data, such as initialization vectors, and public parameters and constants used by encryption schemes.

Who we are

The Information Technology Laboratory (ITL) is a major research component of the National Institute of Standards and Technology (NIST) of the Technology Administration, U.S. Department of Commerce. We develop tests and measurement methods, reference data, proof-of-concept implementations, and technical analyses that help to advance the development and use of new information technology. We seek to overcome barriers to the efficient use of information technology, and to make systems more interoperable, easily usable, scalable, and secure than they are today. Our web site is http://www.itl.nist.gov/.

Users must understand how their cryptographic products work to ensure that the keying material needed to recover data from their systems and applications is appropriately and securely backed up for key recovery. In some products, special key recovery features have been designed into the product to make key recovery comparatively easy; for example, many Certification Authority (CA) products build in a feature for the CA to retain an encrypted copy of encryption keys and access those keys under specified security controls. In other cases, users may need, for example, to export keys from hardware cryptographic modules and store them in a safe place.

When sensitive data is backed up, the backups themselves are sensitive data and must be protected. However, if the sensitive data is encrypted, *then backups of the sensitive encrypted data may not require additional confidentiality protection, provided that the keying material needed to access that encrypted data is adequately protected (e.g., encrypted under a different storage encryption key and/or separated from the sensitive data).* Users are cautioned that the protection mechanism used to protect the key needed to decrypt the sensitive data needs to be carefully assessed as to the security it provides. For example, some file encryption products may store the decryption key, encrypted using a password, with the encrypted data or may generate the decryption key directly from a password. If the encrypted backup of the key and data is stolen, it may be possible to conduct an "offline" password guessing attack against the encrypted data, since passwords are often easy to guess.

Informal key recovery by ad hoc user backup of keys may be appropriate when personal files, individual working drafts, and the like are encrypted, or when the loss of that data would not seriously impact the mission of the agency. However, where important data is encrypted, and either the loss or compromise of that data would significantly affect the mission of the agency, a formal Key Management Policy should be developed detailing policies for the use and handling of keys and identifying the keys that are subject to key recovery. For each system that uses cryptography, a Key Management Practices Statement should be developed, detailing the specific key generation, protection, maintenance, use, and key recovery procedures employed.

NIST is now developing a key management guidance document that will provide detailed guidance on how keys should be managed, including the key recovery aspects.

Disclaimer: Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.

U.S. DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
100 Bureau Drive, Stop 8900
Gaithersburg, MD 20899-8900

Official Business
Penalty for Private Use $300
Address Service Requested

PRSRT STD
POSTAGE & FEES PAID
NIST
PERMIT NUMBER G195