3.1.7 Data Retention Facts

Data retention policies define how information in your possession is maintained and for how long. The key point to remember is that different types of data must be retained for different lengths of time based on legal and business requirements.

> Litigation and criminal investigations are key factors that influence the data retention policy in most organizations.

Data retention policies also typically describe procedures for:

- Archiving information
- Destroying information when the retention limit is reached
- Handling information involved in litigation

Review all of the different types of information used in your organization and develop a policy that defines how long different types of data are retained and destroyed when the retention period is past. Record this information in a clearly written policy. Having a written policy and ensuring everyone in the organization follows it protects you from accusations of destroying evidence. Adhering to your data retention and destruction policy protects you and your organization. Never allow selective or arbitrary information destruction. It might make it appear that you are trying to hide evidence and could expose you to potential criminal charges.

> Never destroy information after it has been subpoenaed or if you have reason to believe that it may be subpoenaed. Destruction of evidence and obstruction of justice are serious crimes that could result in jail time.

Other benefits of implementing a data retention and destruction policy include:

- Reduced cost of discovery requests in the event of legal action. Responding to discovery requests can be time-consuming and costly. If old material has been destroyed, discovery costs are minimized.
- Reduced exposure during discovery. Minimizing the amount of electronic material an organization keeps reduces the amount of information that could expose an organization to potential litigation.
- Reduced hardware and software requirements for storing old data.

Sample data retention rules could include the following:

- Delete email messages after 90 days.
- Keep tax-related information for seven years. This timeframe should be defined by the applicable taxation authority. For example, the United States Internal Revenue Service requires tax information to be retained for seven years.
- Keep employee records for four years after an employee leaves the organization.
- Keep integral research, design, or patent documents for 25 years.
- Keep contracts with vendors and partners for five years after a contract has ended.
- Delete employee files after one year.

After creating your written data retention policy, use information classification labels to identify which retention policy rule is to be applied to specific data. Using classification labels allows you to use software tools to automate the data retention and destruction process.

All information should be destroyed before being disposed of. Simply deleting files can leave sensitive information behind.
