Strategy Report

Why You Should Consider an Electronic Data Management Policy

It is estimated that 97% of business data is now exclusively stored electronically.

An organization's records management policies should reflect the characteristics of electronically stored information. Electronic records are easily created, easily copied, widely distributed and are stored in numerous devices, including computers, personal digital assistants and cell phones. Electronic records are hard to delete permanently. The embedded metadata typically preserves information about creation, revision and authorship. People treat electronic records more informally, saying things in e-mail they would never write in a formal letter.

The temptation is to archive every electronic record. This is often not the best solution. It may mean that an organization has no satisfactory way of accessing its own business information. From a legal standpoint, the organization risks non-compliance with its legal obligations and, should the organization face litigation, the "store everything" approach can be costly.

Organizations should consider a records management policy dealing systematically with creation, retention and destruction of records. It makes good business sense to have effective control of records, and can avoid potential legal issues associated with poor records management:

- The risk of destroying records an organization is legally required to retain. Every organization has to comply with multiple records retention requirements.
- The risk of retaining records an organization is legally required to destroy - privacy legislation typically requires that personal information should only be accessible to those who need to review it and should be destroyed once its purpose has been satisfied.
- The risks in a litigation context - 1) the organization may not have retained, or may not be able to locate, required documents when faced with litigation; 2) if unnecessary documents have been stored, it can be costly and burdensome to identify relevant records in the discovery process (depending on the circumstances, courts may require individual review of electronic documents); and 3) an organization may be exposed to claims that it improperly destroyed records when it knew that litigation or regulatory action was imminent.

A records management policy needs to be organization-specific, but the general rule is an organization should retain only the information it needs for only as long as it needs it. Specifically:

Creation of records - E-mails, in particular, create problems. Employees treat them as the equivalent of phone calls. Implement a clear e-mail policy and communicate it to employees.

Record retention and destruction - Incorporate legislative and regulatory requirements. In the litigation context, courts have looked to see if the destruction of records was in accordance with an established policy of purging records.

Confidentiality - Establish procedures to prevent inadvertent disclosure of confidential or privileged information.

Compliance mechanism - Incorporate a process for auditing compliance. In the litigation context, you may be worse off having a policy that was not complied with than having no policy at all.

The litigation hold - Provide a process to halt destruction of records when litigation or regulatory action is reasonably anticipated. If there is no procedure for a litigation hold, the organization risks court sanctions.

Stanley Martin, *partner, conducts a litigation practice at Fasken Martineau, Vancouver.*