AltiusIT

Managing Information Technology (IT) Risks

Introduction

Organizations are finding that the fast paced Information Technology (IT) industry is a double edge sword. While improving operational efficiencies, employees are exposing their businesses to even greater risks. This article identifies various risks and how risk assessments help organizations identify, manage, and reduce their risks.

Risk Scenarios

Imagine going in to work one day and finding that you have been summoned to appear in court. You find that a lawsuit has been filed against your organization. After some research by your legal staff, you are told that one of your employee's E-mail messages is being used against you and will appear as evidence in your upcoming trial. Imagine that when you read your employee's E-mail message for the first time, you discover that the E-mail contains sensitive and confidential information about your organization. What can your organization do to avoid future risks?

Organizations are finding that they need to change the way they handle and maintain their electronic records and communications. Many are planning to use IT to manage their risks and potential liabilities by securing and managing their electronic documents and confidential communications.

Document Management

Information must be managed and many different types of information exist within an organization. In the past, organizations maintained large volumes of paperwork in office filing cabinets and off-site warehouses. Access to information required employees to sift through files trying to locate the needed records.

Many organizations improved their access to information through the use of Information Technology solutions that automated the document storage and retrieval process. Through IT solutions such as electronic mail and electronic scanning and filing, documents could be located in minutes or even seconds. No longer did it take days or weeks to find the requested information.

In providing immediate access to information, a new risk emerged. While documents were accessible for internal reference purposes, they were also available to be subpoenaed. A second problem also arose. With traditional file cabinets, organizations tended to have only one version of a document on file. However, with electronic filing, an organization could have word processing documents, E-mail messages, electronic fax transmissions and other types of electronic communications available at a moment's notice.

Organizations now realize the implications of maintaining electronic communications and the need to better manage these documents through a formalized document management archival and destruction procedure.

To manage risks, document management and electronic communications procedures should be developed at the highest executive levels and pushed down to lower levels within the organization. Enforced company wide, document management considers information stored internally, on tape backup media, on the Internet/Intranets, as well as communications with outside business contacts.

Confidential Communications

In addition to managing their documents, organizations must be especially concerned about their confidential communications. These types of communications may occur within an organization or may also include communications with outside business contacts.

To manage their risks, organizations will use IT to better protect their electronic communications. Confidential documents and communications will be encrypted to protect information. While these steps are already being used by some organizations, others are finding that more extensive procedures need to be implemented.

Electronic communications via e-mail will receive special attention. Employees typically have found it beneficial to store electronic versions of e-mail messages. Management tends to believe that these messages may pose more harm than good. As a result, management may dictate that this type of correspondence be removed after a period of time. While many organizations have controlled the archival and destruction of E-mail messages within their organization, most have yet to address electronic communications with outside contacts.

To manage their risks, organizations will implement solutions that more fully address confidential communications and e-mail. For example, management can dictate that e-mail messages expire a pre-determined number of days after the initial transmission of the message. This provides management with the peace of mind knowing that their risks are properly managed. Retention policies should be decided and approved by organization management before they are implemented by IT. The technical impact includes:

- Electronically stored documents
- E-mail
- Instant messaging
- Content management
- Backup systems

E-Discovery Primer

E-discovery refers to the process of finding and producing electronic documents in response to litigation or regulatory requirements. Federal Rules of Civil Procedure require organizations to maintain, and produce on demand, electronic communications and records.

IT has many e-discovery related responsibilities:

- Review documents and e-mail communications to identify the types of information that need to be managed.
- Review document and e-mail archiving policies to ensure the electronic information is retained for the appropriate period of time.
- Determine if information is stored locally even if archiving and destruction procedures remove information from central archives.
- Review e-discovery tools and services to help speed the recovery of data from backup tapes or other media. Such tools can shorten the time required to retrieve relevant information.

Sensitive Communications

Business executives in the future will be expected to take more of a proactive role by actively controlling and monitoring electronic communications. IT systems will be configured to restrict the sending or receiving of messages that may contain questionable material.

By configuring software applications to look for certain keywords or phrases, outgoing E-mail correspondence can be stopped before the message has left the sender's desk. Questionable incoming messages may be routed to a special pending mailbox where they will be held pending a third party review.

By configuring software to look for certain keywords or phrases, an organization can prevent questionable communications that may result in sexual harassment lawsuits or other types of litigation.

Summary

Each organization has a unique environment that makes it difficult to protect against new and emerging threats. Network security audits help organizations identify, manage, and reduce their risks.

Publication Information

Altius IT is a security audit, security consulting, and risk management firm. We are certified by the Information Systems Audit and Control Association (ISACA) as a Certified Information Systems Auditor (CISA), Certified in Risk and Information Systems Controls (CRISC), and Certified in the Governance of Enterprise Wide IT (CGEIT). For more information, please visit www.AltiusIT.com.