COA[1] Paper
Information Lifecycle Management

Introduction

Many information assets within an organisation have an associated value relative to the business impact of an incident or threat that affects the confidentiality, availability, authenticity or availability of the information. The threat model for information stored locally, within network perimeters, is different that of information shared in collaborative, de-perimeterised environments. The former allows an organisation to control access to information within a secured perimeter for a specified set of users, while the latter allows information "into the wild" where there is no perimeter in which to enforce access control and no finite set of users to control access for.

It is therefore essential that information is correctly and accurately classified to identify the organisations and individuals that should have access to it as well as the data handling requirements such as secure storage and safe disposal that are relevant to the information content.

It is also crucial that the confidentiality, integrity, authenticity and availability of the information are categorized are made clear in order to inform information users how to secure information in situ, use and transit outside of the secure perimeter.

The Problem

Shared information has an associated value to its organisation. Where information is shared in collaborative, de-perimeterised environments, the information content should be correctly labelled with information protection requirements according to an Information Classification Scheme and Impact Sensitivity Categorization, as defined in the Jericho Forum papers with the respective titles.

Information can often have a temporal aspect. For example, financial results can go from top secret to public domain overnight. Information Classification and Impact Sensitivity Categorization should be periodically reviewed and updated to reflect the current sensitivity of the information. Access controls should be modified in light of any changes to information classification.

The Information Classification, Impact Sensitivity Categorization, Access Control Requirement definition/modification processes, together with policy for the creation, storage, transfer, update and deletion of information require an entire Information Lifecycle Management (ILM) process which should be a continual cycle of analysis.

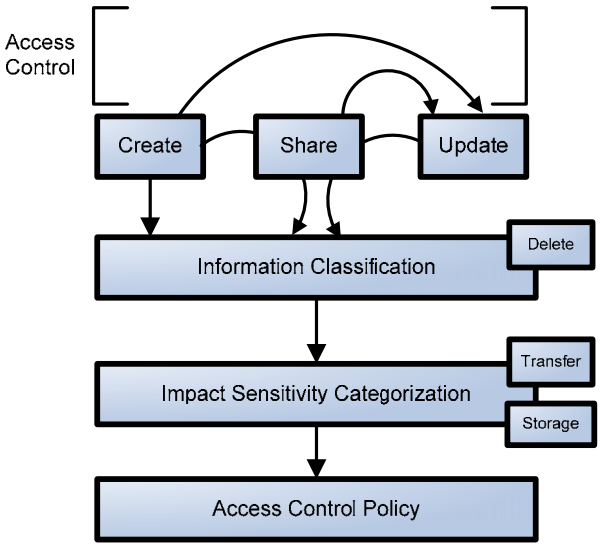
[1] Collaboration Oriented Arcvhitectures paper, and COA Framework paper – available at http://www.opengroup.org/jericho/publications.htm

Why Should I Care?

The way in which people work is changing. Web 2.0 is bringing a cultural change and business drivers are forcing organisations to collaborate. At the same time, changes to the Data Protection Act 1998 are putting personal responsibility for data losses and exposures with the data controller. It is more important than ever to maintain strict control over information, while at the same time allowing information to move into an environment over which organisations currently have minimal control. Organisations must begin to classify and categorize information that is to be shared in de-perimeterised environments in this way to maintain control over it and comply with legislative control, maintain control over the intellectual property of the information, and maintain control of their sensitive business information.

Recommended Solution

The illustration below details the ILM Process model for use in COA, defining the actions that can be taken on information at any one time, the options available while taking those actions and the path an individual should follow to ensure the information remains secure throughout its lifetime from creation to deletion.



ILM Process Model

Creation

A lot of information is created as part of the everyday business process within organisations. Upon creation, the creator must consider the content of the information they are creating and make a decision as to whether or not it requires access control. If not, then its lifecycle can continue without applying the ILM Process. If it is, the Information Classification, Impact Sensitivity Categorization and Access Control Policy Definition stages of the process must be performed.

Storage

Information must be stored appropriately to reflect the information protection requirements defined by the Information Classification and Impact Sensitivity Categorization stages. Encryption is not mandated but if the information is highly classified or has high impact

sensitivity then confidentiality assurance must be considered. The physical location of the storage devices and the encryption of information are example considerations.

Information Sharing

Information shared in collaborative, de-perimeterised environments is subject to a different threat model to information stored locally. In light of this the Information Classification, Impact Sensitivity Categorization and Access Control Policy Definition stages of the process must be performed before sharing the information, even if this has already been performed on creation of the information.

Data Transfer

The information transfer protocol between collaborating parties should take account of the information protection requirements as defined by the Information Classification and Impact Categorization stages. Encryption is not mandated but if the information is highly classified or has high impact sensitivity then confidentiality assurance must be considered. Endpoint compliance and the encryption of information in transit are example considerations.

Update

If the information is updated, the updater must consider the content of the information they are adding/updating and make a decision, using the Information Classification Scheme and Impact Sensitivity Categorization processes, as to whether or not the changes present additional and/or modified information protection requirements. Changes in Access Control Policy and data transfer security are examples of such protection requirements that may change due to modified information content.

Deletion

Deletion of the information should reflect its classification and impact sensitivity labels. If the information is labelled as having to be securely destroyed then just placing it in the system "Trash" is not acceptable.

Information Classification[2]

Information that is shared in de-perimeterised environments must be accurately labelled with information protection requirements according to the sensitivity of the content within the information resource in terms of a risk-based assessment of the business impact of an incident or threat.

The information creator or individual intending to share the information in a collaborative, de-perimeterised environment must consider the threat to the business if the information were accessed and/or modified by individuals with an identity outside of a particular domain. This could be the internal organisation, external business community or named specific individuals, details of which must be specified in the Information Classification Scheme for the organisation. The Jericho Forum paper titled Information Classification defines a positional scheme based on the G8 Traffic Light Protocol.

Information handling requirements, legality and temporal aspects must also be considered at the Information Classification phase. Secure destroying of information; clear ownership rights; changes in classification after a particular date and time; and corporate governance constraints are examples of the detail that should be evident from the labelling process.

If the information requires classification according to the Information Classification Scheme, the information must be correctly labelled.

[2] See also Information Classification paper, Jericho Forum publication, available from http://www.opengroup.org/jericho/publications.htm

Impact Sensitivity Categorization

Information must be labelled with an Impact Sensitivity level based on the measures of Confidentiality, Integrity, Authenticity and Availability required to adequately protect the information in situ, use and transit. The Jericho Forum paper titled Impact Sensitivity Categorization proposes a six-level impact sensitivity scale that represents the impact magnitude should the protection measures not be effectively deployed.

The creator or individual that is intending to share the information in a collaborative, de-perimeterised environment must conduct an Impact Sensitivity analysis to determine the controls required to maintain information assurance in a de-perimeterised environment in relation to the Confidentiality, Integrity and Availability requirements of the information.

Access Control

Authentication and Authorisation should be applied to principles requesting access to information. The Jericho Forum paper titled Control Stratification details a set of levels for which trust in an identity can be assured.

Appropriate access control technology should then be used to enforce the authorisation response. The de-perimiterisation issue makes many of the current technologies that rely on perimeter security to enforce controls inappropriate for use in COA. The Jericho Forum paper titled Electronic Information Protection & Control (EIPC) details the digital management of rights to access information and includes a position on how to control access to information in collaborative, de-perimeterised environments.

Access Controls should be reflective of and responsive to the information security requirements defined in the Information Classification and Impact Sensitivity Categorization stages.

Background & Rationale

Not all information carries the same value and associated information protection requirements. Consequently, there must a way of classifying information so that the different and most important information protection requirements can be identified for any given piece of information by anybody accessing or sharing it. The classification scheme should be concise and clear so that it can be applied quickly and accurately by anybody creating or sharing information that is of value to an organisation.

Access to some information may be limited to specific identities. These identifies could be public, domain specific, organisation-wide, departmental or even specific individual details. Other information may be limited based on environmental conditions such as worldwide location while requesting access or endpoint compliance of the machine requesting access.

Data handling is often an important issue. Simply deleting information does not destroy it so controls such as electronic shredding could be mandated on the most sensitive information. Likewise, secure and tamper evident data transfer and storage protocols may also be enforced for particularly sensitive information.

Information Classification Schemes and Impact Sensitivity Categories should reflect the requirement for these controls in their choice of labels and allow an organisation, data controllers in particular, to identify and make clear the information protection requirements of their information through the assignment of such labels to information, so that internal and external users know how it must be handled and controlled throughout its lifecycle.

Challenges to Industry

Shared Taxonomy

Getting taxonomy for the entire ILM process and all of its components, including Information Classification and Impact Sensitivity Categorisation to be appropriate and usable between organisations is essential. The taxonomy used by one organisation must be able to be understood and interpreted by all other collaborating organisations in order to adequately protect the information according to its organisation-specific requirements.

Enforcement

The ILM process must be enforced for all information shared in de-perimeterised environments to ensure information security outside of the perimeter. The key driving principle in COA audit is transparency between partners. Creating an audit trail of who created, accessed, updated and deleted information and maintaining an accurate and complete trail of changes to information classification and impact sensitivity categorisation labels is essential to meeting the rigor required for forensic evidence in law.

The Way Forward

Organisations need to begin trialling Information Classification and Impact Sensitivity Categorizations schemes as part of their internal operations and then moving the successful ILM process model into a collaborative domain. De-perimeterisation is happening; Data Protection Laws are becoming more powerful and will soon carry civil penalties; business drivers are forcing organisations to collaborate. It is essential that the ILM process begins to become part of everyday business activity.