Asset and Data Management

Getting Started

It is well known that you cannot secure what you do not know exists. Asset and data management is all about discovery, ownership, value, acceptable use, protection, and disposal of information-related assets. Assets can be tangible, like hardware, or intangible, like software and data. Whether you are with a small or large institution, a good place to start is:

1.Know What You Have
2.Know Where It Is
3.Know Who Owns It and Who Maintains IT, and
4.Know How Important It Is to The Institution.

Develop the 4 "knows" for a great start and, perhaps, successful finish to your asset and data management initiative. Each of the "knows" are expanded upon below.

Know What You Have

1.Review potential institutional sources of information assets. A holistic perspective that includes data centers, hardware, software, and data may require various sources including:

a) Institutional asset inventory reports from departments responsible for purchasing and equipment asset inventory.
b) Institutional information security risk assessments.
c) Business Continuity and Disaster Recovery plans (good source for critical systems).
d) Visit your institution’s CIO and data center management and discuss what information resources are under their custody.
e) Visit major stakeholders (senior staff, administrative department heads, etc.,) and discuss what information systems and data their department handles.

2.Create a spreadsheet of the items.

a) List the assets for each category.
b) Define distinct categories for the types of assets in your institution (e.g., infrastructure, data center hardware, information systems/applications, data).

Know Where It Is

1.Record the physical location of the asset in your spreadsheet. You may want to divide them into Local and Hosted.

a) Include under Local institutional brick and mortar physical locations such as classrooms, data centers, labs, or offices. Example: the location of collaborative research materials on a file share may be Primary Data Center X.

b) Include under Hosted third-party vendor data centers and other remote locations not owned by the institution. Example: the location of the learning management system is Vendor X data center located in Address.

Know Who Owns It and Who Maintains It

1.Identify and record in your spreadsheet the Owners and Custodians for each of the assets listed in your spreadsheet. Most of the times, the individuals responsible for the security of the asset and ensuring compliance are not the same as the individuals responsible implementing security controls and day-to-day operations.

a) Example 1 (Local): the owner of the Student Information System may be the Registrar and the custodian may be the institution's IT department.
b) Example 2 (Local): the owner of the network switches may be the Director of Office of Network and Telecommunications and the custodian may be the same department.
c) Example 3 (Hosted): the owner of the Learning Management System may be the Dean of the School of Business and the custodian may be Vendor X.

Know How Important It Is to The Institution

1.Review the federal or state laws, regulations, rules or institutional policies that require protection of information resources. These could be FERPA, HIPAA, or a state law governing social security number use.

2.Review your institution's Data Classification Policy.

3.Determine from your sources from Step 1 whether your institution's assets are classified in accordance with the Data Classification policy. If not, this Data Classification Toolkit may be helpful to you in getting started.

a) Create a simple classification schema (e.g., Public, Restricted, Confidential).

4.Create a criticality rating for the assets. For example (highest to lowest):

- 1 – critical is always available and protected
- 2 – very important this asset is available and protected
- 3 – important if this asset is available and protected
- 4 – good if this asset is available with minimal protection

5.Record in your spreadsheet the asset classification and/or criticality ranking.

a) Example 1: The LMS system has a rating of 2.
b) Example 2: Student Records are Confidential and have a rating of 1.

At this point, you are ready to determine whether institutional assets are protected according to their classification and importance.

Overview

An asset is defined as "an item of value". (Source: Merriam-Webster's Online Dictionary) Asset and data management is based on the idea that it is important to identify, track, classify, and assign ownership for the most important assets in your institution to ensure they are adequately protected. Tracking inventory of IT hardware is the simplest example of asset management. Knowing what you have, where it lives, how important it is, and who's responsible for it are all-important pieces of the puzzle.

Similarly, an Information Asset is an item of value containing information. The same concepts of general asset management apply to the management of information assets (e.g., data). To be effective, an overall asset management strategy should include information assets, software assets, and information technology equipment. In addition, the people employed by an organization, as well as the organization's reputation, are also important assets not to be overlooked in an effective asset management strategy.

An institution should be in a position to know what physical, environmental or information assets it holds, and be able to manage and protect them appropriately. Important elements to consider when developing an asset and data management strategy are:

- Inventory (do you know what assets you have & where they are?)
- Responsibility/Ownership (do you know who is responsible for each asset?)
- Importance (do you know how important each asset is in relation to other assets?)
- Establish acceptable-use rules for information and assets.
- Establish procedures for the labeling of physical and information assets.
- Establish return of asset procedures (do you have an employee exit procedure?)
- Protection (is each asset adequately protected according to how important it is?)

Responsibility for Assets

Objective: To ensure adequate protection of organizational resources, all assets should be accounted for and each should have a designated responsible party.

Asset Inventory

Do you know what assets you have and where they are?

In order to effectively manage an organization's assets, you must first understand what assets you have and where your organization keeps them. Some institutional asset examples are IT hardware, software, data, system documentation, and storage media. Supporting assets such as data center air systems, UPS's and services should be included in the inventory. All assets should be accounted for and have an owner. If improperly managed, assets can become liabilities.

So where do you begin?

Categorize your assets

Begin by defining distinct categories of the types of assets in your institution. Each category should have its own inventory or classification structure based on the assets that category may contain.

(Category: Data Center Hardware)

Create a list of assets for each category. Creating a list of an institution's assets and their corresponding locations is the beginning of your inventory. Often, the process of doing so helps identify additional assets that previously had not been considered.

(Category: Data Center Hardware; Asset: Core Network Switches)

Add a location for each asset. Location could be a brick and mortar physical location such as a classroom, data center or office. It could also be collaborative research materials on a file share or financial information stored in a database.

(Category: Data Center Hardware; Asset: Core Network Switches; Location: Einstein Bldg., Rm. 0001)

Because assets can be many things and serve multiple functions, there will likely be more than one inventory process or system used to capture the range of assets that exist at an institution. Make sure you connect with other areas to see what form of hardware inventory already exists. Don't start from zero. Each inventory system should not unnecessarily duplicate other inventories that may exist.

Asset Responsibility/Ownership

Do you know who is responsible for each asset?

Once you have begun to capture an inventory of the potential assets and their locations, start identifying the responsible party, or parties, for each asset. An owner is a person, or persons or department, that has been given formal responsibility for the security of an asset. The owner(s) are responsible for securing asset(s) during the lifecycle of the asset(s). At this juncture in the exercise it is important to understand the distinction between the terms "owner" and "custodian" of assets.

The custodian is responsible for ensuring that the asset is managed appropriately over its lifecycle, in accordance with rules set by the asset owner. The custodian is often a subject matter expert (SME) or "owner" of the business process for a particular information asset. An owner of an information asset, Data Owners if you will, have direct operational responsibility for the management of one or more types of data. Think of it in terms of an information security department. You have the "owner", the person responsible for interpreting and assuring compliance. That would be the Director or CISO. Then there is the custodian(s), the person(s) responsible for the day-to-day operations and management of the tools and processes that protect the information assets.

Identifying the owners will help determine who will be responsible for carrying out protective measures, and responding to situations where assets may have been compromised. You will also quickly realize when it isn't clear who the appropriate responsible party is or when shared responsibility may be an issue.

> (Category: Data Center Hardware; Asset: Core Network Switches; Location: Einstein Bldg., Rm. 0001; Owner: Director Thomas Stoltz Harvey)

The owner(s) of the assets should be able to identify acceptable uses or provide information on which institutional policy governs its acceptable use. Work with the responsible owner, if need be, on acceptable uses. The acceptable uses should include items such as who assumes the risk of loss, gives access to the asset and how a critical asset is kept functional during or after a loss. Policies governing the use, preservation and destruction of hardware may originate from your asset management office. Many institutions also find it helpful to document expectations for the acceptable and responsible use of information technology assets in an Acceptable and Responsible Use Policies.

Identifying an owner, or responsible party, for physical hardware or software is relatively easy. Information assets may be a bit more difficult to identify, classify, and apply ownership.

Physical and Environmental Asset Importance

Do you know how important each asset is in relation to other assets?

All assets add value to an organization. However, not all assets are created equal. Gaining a clear understanding of the relative importance of each asset when compared to other organizational assets is an essential step if you are to adequately protect your assets. The importance of an asset can be measured by its business value and security classification or label.

Create a rating system for the asset. It can be as simple as (highest to lowest)

- 1 – critical is always available and protected
- 2 – very important this asset is available and protected
- 3 – important if this asset is available and protected
- 4 – good if this asset is available with minimal protection

Building on the previous example and adding a rating system, it would look like

> (Category: Data Center Hardware; Asset: Core Network Switches; Location: Einstein Bldg., Rm. 0001; Owner: Director Thomas Stoltz Harvey; Rate: 1 (Critical))

A student computer lab machine, depending on its location, may have a lower score given it is good that the asset is available. The computer lab machine may be protected with anti-virus.

Acceptable Use of Assets Associated with Information

Have you defined, documented and communicated the acceptable use of assets?

After going through the asset inventory, categorization, and ownership identification, ensure there is documented policies regarding the acceptable use of assets. Define, and document, the rules that clarify the acceptable uses of assets associated with information and information processing facilities. It is important, once the rules are clarified, that appropriate controls are implemented and the security requirements are communicated. Target the communication of security requirements to employees and, if appropriate, third parties who may use these assets. Accountability is key. Asset owners should be responsible and accountable, even if the owner has delegated responsibility, for their use of facilities and resources.

Return of Assets

Do you have employee exit procedures that include return of institutional assets when employment is terminated?

It is critical that institutions protect their information on equipment of employees when their employment is terminated. Make sure all relevant information that will be needed by the institution is preserved, but all information on the asset is erased. Develop an employee exit checklist that addresses the return of all institutional assets, physical or information, before the employee's last day. There are, of course, emergency situations dealing with immediate termination that may not lend itself to a measured checklist. Create a simple checklist for those instances as well. Get to know a resource in your HR area and work with that resource to incorporate physical and electronic assets at termination.

As stated before, assets can be a variety of items. Employee knowledge is also an information asset to the institution. Preserve their relevant knowledge, document, before the individual leaves the institution and ensure that knowledge is in the institution's possession. Once again, use the checklist to incorporate this aspect of asset return. A sample may include:

- Employee has returned all computing equipment to IT.•IT will preserve the information on the equipment by copying to external drive or employee group share file server. Preserved information will be given to the employee's supervisor.
- Employee has transferred all institutional information from his/her personal equipment and given that to their supervisor.
- Employee rights to information assets have been terminated as of this date.
- Employee knowledge transfer has occurred.

Don't forget about the contractors, consultants or any other external third party upon termination of contract or agreement. The same rules apply. You may wish to have a separate asset security checklist for all external agents and ensure this information is part of their contract or agreement.

Information Classification

Objective: To appropriately protect various kinds of information, implement a classification scheme that states the relative importance of each type of information to the organization, as well as an appropriate level and method of protection for each.

Data Protection and Privacy of Personal Information (Records Management)

The data every institution uses in its mission of teaching is a valuable resource that needs to be protected commensurate with how it is classified. Students and staff entrust the institution with a given data set and there is an implied bargain that the data so entrusted will be protected from any use or disclosure other than as agreed to when the data was given.

To do this, each institution has to govern the data it uses so that it will be received, made, used, stored, shared, or destroyed in a purposeful manner which recognizes the pact to protect data in an institution's daily mission. Areas to consider in a data governance program include:

- Sensitivity Level. An institution should be classifying data as to sensitivity to assure that proper security protection is in place appropriate with the given data set. EDUCAUSE has excellent materials, including the Data Classification Toolkit.
- Retention Period. Consistent with records management practices, an institution needs to be aware of the period in which data is to be retained, to assure that data's availability and integrity for that retention period.
- Data Utilization. In every part of an institution that controls a given data set, appropriate procedures for how that data is utilized must be established. This includes access restrictions, proper handling, logging, and auditing.
- Data Back-up. How an institution creates back-up copies of data and software is a critical element. Procedures need be in place that memorialize and verify the implementation and inventory of back-up copies.
- Management of Storage Media. Processes to ensure proper management of storage media, including restrictions of types of media, audit trails for movement of media, secure disposal of media no longer in use, and redundant storage.
- Electronic Data Transfers.
- Disposal of Media. Visit the Guidelines for Information Media Sanitization for current practices and recommendations.

Information Asset Importance

Do you know how important each information asset is in relation to other assets?

Information assets may not be equally important, nor equally sensitive or confidential in nature, nor require the same care in handling. One common method of ascertaining the importance of assets is data classification. Information assets should be classified according to its need for security protection and labeled accordingly.

So where do you begin?

Start with federal or state laws, regulations, rules or institutional policies that require certain information assets be protected. These could be FERPA, HIPAA, or a state law governing social security number use.

Pick a classification metric. Keep it simple. You may want to use something like (lowest to highest)

- Public, Restricted, Confidential

Perhaps your inventory of information assets might look like

> (Category: Information; Asset: Student Records; Location: Banner Cluster 1, database sis_prod; Owner: Dean of Admissions; Rate: 1 (Critical))

Asset Protection

Is each asset adequately protected according to how important it is?

Different assets have different impacts on the continuity and reputation of the organization. Once you have determined the importance of your various organizational assets, you can begin the process of determining how best to protect them.

Many methods are employed to protect assets, ranging from legislative mandates (and their enforcement) to policies to technical security controls. Additionally, assets must be protected throughout their life cycle, from creation or purchase through final disposal or long-term storage.

Protection measures range from addressing purchasing controls to managing access by appropriate personnel to ensuring adequate physical security for assets throughout their lifetime.

Some institutions have established Data Stewardship policies to help ensure responsibilities for protecting data are effectively accomplished. It is important to note that data custodians/stewards are the decision-makers when it comes to accessing records. There needs to be a process in place for requesting access to both static and live data. The process/policy should include contract language or review to determine what happens to institutional data when a contract with a vendor is no longer in force. The data custodians/stewards can work with you to help develop policies if none are yet in place.

Other institutions conduct regular security assessments of assets considered to be critical for the functioning of an institution. Institutions may also address asset protection through physical security measures, or through background checks for newly hired and continuing personnel.

Labeling of Information

Do you have your information and physical assets labeled?

Your institution may already have property control of assets where items over a certain dollar amount are automatically tagged with a unique, usually numeric, identifier by Property Control. If not, create one yourself. Use your newly created inventory of assets to assign a unique identifier to each one. Prepare labels that are easy to recognize and sturdy, and attach them to a visible place on the equipment. Make sure you clarify when labels should not be used on equipment. This could be based on dollar amount or the level of risk you've assigned to the asset.

Information needs labeling as well. Develop your information labeling procedures based on the data classification schema you developed previously. Metadata is a common type of information label. Do be careful how you manage the information you may have labeled as restricted or confidential. Because of the labeling, be careful how you manage restricted/sensitive or confidential information. It is much easier to steal or misuse when the assets are easy to identify.

Handling of Assets

Is information being handled and protected according to its classification?

Now that you have your assets identified, classified and labeled, you will need to develop procedures for handling assets associated with your information and information processing facilities. It is important that your asset handling procedures respect and reflect how you classified it. Ensure that

- Information is handled and protected according to its classification. This includes sharing with external entities.
- There are procedures to control classified information. Clarify how yours, and perhaps others', classifications should be interpreted.
- Information is stored, processed, transmitted and copied according to its classification. Copies should get the same protections.
- Access restrictions are designed for each level of classification. Restrictions must meet protection requirements.
- There is a formal record of the authorized recipients of the assets. Specify who the authorized recipient should be. Label media copies appropriately.

All of the above bullet points can be incorporated into one procedural access handling document. Remember, keep it simple so others will be able to understand and comply with the requirements. Hold a session with your information and physical asset owners so they can help you define the requirements. It's important everyone feels ownership for this process.

Media Handling

Objective: To prevent business disruptions due to the unauthorized disclosure, modification, removal or destruction of information and information technology resources.

Management of Removable Media

Integrate necessary controls to manage media items, whether tapes, disks, flash disks, or removable hard drives, CDs, DVDs, or printed media, to ensure the integrity and confidentiality of university data. Guidelines should be developed and implemented to ensure that media are used, maintained, and transported in a safe and controlled manner. Handling and storage should correspond with the sensitivity of the information on the media. Procedures to erase media if no longer needed, to ensure information is not leaked, are also important.

Disposal

Procedures for handling classified information should cover the appropriate means of its destruction and disposal. Serious breaches of confidentiality occur when apparently worthless disks, tapes, or paper files are dumped without proper regard to their destruction.

- Guidelines for Information Media Sanitization

Information Handling Procedures

Procedures for handling and storage of sensitive information, together with audit trails and records, are important. Accountability should be introduced and data classification and risk assessments performed, to ensure that necessary controls are applied to protect sensitive data. Appropriate access controls should be implemented to protect information from unauthorized disclosure or usage. Systems are also vulnerable to the unauthorized use of system documentation; much of this type of information should be regarded and handled as confidential. Security procedures, operating manuals, and operations records all come into this category.