A Brief Introduction for UN Folks on Information Security Classification

Information Security Management

Herrmann, Heiko

3/15/2012

Unclassified/Public

Know your information and what its value depends on. Spend as much money as required but not more than necessary to protect information and to ensure that it is available and kept correct.

A Brief Introduction for UN Folks on Information Security Classification

Information security classification aims to categorize information assets (e.g. electronic and non-electronic documents, business records, email, databases) into security categories. It can be considered a subset of information classification.

The objective of information security classification and categorization is to identify the level of protection required as well as the appropriate level of efforts to maintain the information integer and available. In order words, by the book there are three information security categories: SENSITIVITY, AVAILABILITY and INTEGRITY.
In practical implementations, however, sensitivity classification often dominates and is the only classification scheme used, respectively. Some of the reasons why this is the case; are given later in this document.

Protection measurements as well as efforts to ensure integrity and availability translate directly into costs. Protecting information costs money, the investment and operation of high availability systems for information, which has high availability requirements also costs money; and so does the design and implementation of data integrity protection mechanisms for information that has high integrity requirements.

There is a broad spectrum of potential tangible and intangible losses related to information incidents. Breach of confidentiality, integrity or unavailability of information could result in major loss of reputation, customers or revenue, lawsuits and reproduction/re-creation costs.

The ultimate objective of Information Security Classification is hence:
Know your information and what its value depends on. Spend as much money as required but not more than necessary to protect information and to ensure that it is available and kept correct.

Why is an Information Security Classification/Declassification Policy/Standard needed?

An Information Classification/Declassification Policy/Standard is the base for the Organization's approach towards implementing the classification. The standard is to ensure that everybody is - literally - on the same page. The policy/standard should deliver the following:

- Definition of roles:
  owners, custodians, users of information - there are typical roles attached to the life-cycle of an information asset and often those roles are overlapping. The information classification policy/standard needs to define and clarify the roles.
- Definition of the classes that the organization is going to use to classify information (how many, which types). Tip: Keep it simple.

- Definition of the criteria for the classes:
  that is one of the most difficult parts. It is not easy to develop very concrete and detailed criteria. But the truth is: the more generic and vague the criteria are, the less useful the policy/standard is.
- Clarification of responsibilities: who (which role) is responsible for doing what and when

Challenges

The implementation of information classification is not simple. A really good Information Classification Policy is able to address or at least to provide guidelines on challenges such as:

- The requirements concerning confidentiality, availability and integrity, which can be quite dynamic.
  For example: The confidentiality requirements of a document can be depending on the timing (e.g. before or after a press release). The availability requirements usually always depend on timing (e.g. conference working papers need to be highly available only shortly before and during the conference).

- Scoping/boundaries
  Often a logical unit of information comprises of smaller pieces of information or data. A file might be comprised of records; a database is comprised of tables and the tables of columns. If one cell in the column of a table of a database contains a confidential piece of information - does that make the database confidential?

- Quantity
  Every day, tons of new information is created. What qualifies a piece of information to be an information asset that is subject to the classification policy?

- The implementation as well as the maintenance of classification and declassification can be expensive.

Information Security Classification in the UN

As mentioned earlier, information security classification schemes for various reasons often only considering the sensitivity/confidentiality aspect - so does ST/SGB/2007/6.

ST/SGB/2007/6 - Information sensitivity, classification and handling - is an UN Secretariat Secretary General bulletin entered into force in February 2007 - and as of today (March 2012) it is still the law of the (UN) land. The objective of the bulletin is to ensure classification and secure handling of information trusted to or originates from the United

Nations. It provides directives on classification principles, classification levels, identification, markings and declassification.

Per ST/SGB/2007/6, the three official UN sensitivity classifications are UNCLASSIFIED, CLASSIFIED and STRICTLY CONFIDENTIAL.

A more recent and practical approach to information classification - still using ST/SGB/2007/6 as a baseline UN policy - is the UN Archives and Records Management Section (ARMS) 's Information Sensitivity Toolkit dated February 2010. The toolkit aims to be a practical and easy to understand guide on topics related to implementation and maintenance of sensitivity classification such as the when, who and how, the handling and the downgrading, declassification and destruction of sensitive information.

An interesting aspect of the toolkit is how it scopes the use of the term *information*.
Quote: *When the term information is used in this toolkit, it refers to information as contained in business records. Security of structured data in information systems is not explicitly covered in this toolkit; nevertheless, some of the concepts covered by the toolkit may be of relevance to IT professionals in the design and maintenance of such systems.* Quote end.

Another interesting detail is that the toolkit is de facto introducing a fourth category: PUBLIC.
Quote: *In contrast, information not meeting one or more of the above criteria should be considered as UNCLASSIFIED (if it is internal information) or PUBLIC (if it is for public consumption). […] It is important to distinguish UNCLASSIFIED (i.e., non-sensitive yet internal) information from PUBLIC information. Although PUBLIC is not considered a classification level, it is important to understand what constitutes PUBLIC information to be able to classify information correctly. PUBLIC information: Information produced expressly for public consumption or that has undergone a declassification process and is now available for public use.* End of quote.

The ARMS Information Sensitivity Toolkit might not be 1:1 applicable in all its details to all UN organizations and agencies. However, it is certainly a very good tool and source for developing a localized, Organization-specifically tailored toolkit that still ensures a homogenized approach towards information sensitivity classification across the UN system

So what about the other two information security categories: availability and integrity ?

At the time of this writing, March 2012, no UN policy or standard presenting an integrated threefold (confidentiality, availability and integrity) classification schema is known to the author.

It should be noted that a complete (threefold) classification schema does significantly increase the complexity of the classification system and thereby of the efforts of its' implementation and maintenance. Adding availability and integrity classes to business information records would create a three-dimensional classification matrix with at least four additional classification levels.

There is another significant difference amongst the categories:
SENSITIVITY/CONFIDENTIALITY can be attributed to a single business information record and, more importantly, the criteria of the classification can be applied to a single information record. In the case of AVAILABILITY though, the criteria to apply availability classification most of the time are derived from a business process or workflow, which the information asset is part of or involved in. In other words: to determine the sensitivity classification one has to look at the content of the information record - whereas to determine the availability classification one has to look at the process (what is the record used for and what is the impact over time if the record is not available (or not integer)).

That difference seems to be contributing to the fact that many organizations have an information security classification policy/standard in place that is in fact a sensitivity-only classification while using availability/integrity classification (only) in the context of business continuity planning and in the context of IT system/service categories (e.g. email system/service = High Availability system/service).

Further UN and non-UN Literature:
For those still having energy and interest to read more on this subject.

NIST Special Publication 800-60: Guide for Mapping Types of Information and Information Systems to Security Categories