Towards an Increased Applicability of the Information Classification Process

Erik Bergström, Informatics Research Centre, University of Skövde

Information classification in short focuses on identifying all information in an organization, classify it and label it. It then serves as input to the risk management. Information classification is a well-established procedure for valuing information from a confidentiality, integrity and availability perspective in an organization. It is a part of asset management in Information Security Management Systems (ISMS), such as the ISO/IEC 27000-series. Several studies highlight the fact that information classification is not a new concept, but still many organizations struggle to complete their information classification (Collette, 2006; Ghernaouti-Helie, Simms, & Tashi, 2011; Glynn, 2011; Hayes, 2008; Kane & Koppel, 2013). In Sweden, it has been mandatory for governmental agencies to do it since 2008 (Oscarson & Karlsson, 2009), but in 2014, 33% of all Swedish governmental agencies didn't do it (Swedish Civil Contingencies Agency, 2014).

We are working with different aspects of the information classification process to enhance the applicability and implementability of the information classification process. This presentation will focus on one of the objectives in the doctoral thesis work, which is to *"develop a security declaration to complement information classification"*.

A complementary approach to information classification is not to classify all information in a process, but rather to classify networks or applications instead of the information. This means that if the network or application contains sensitive data, then it will be classified accordingly, and protected thereafter. This idea draws from work by Fibikova and Müller (2011) and discussions with Region Västra Götaland, and the Swedish Standards Institute. At the moment, work on something called "security declaration" (name is up for discussion) has started, and input from the group could be valuable.

The "security declaration" is supposed to complement the information classification process, and is based on classifying the system that handles the information rather than the information itself. The "security declaration" serves as a basis for system owners rather than information owners, and specifies the technical capabilities of a system in a way that it matches the levels of protection required in the information classification process.

There are many different ways of attacking this problem, and that's where input could be helpful. One way of seeing the problem is to look at security control capabilities such as administrative, logical, technical and physical, or perhaps only technical and non-technical. In that case, the security controls defined in ISO/IEC 27002 could be used as a starting point. Another approach is to base it on functional security requirements from Common Criteria (ISO/IEC 15408). Other ways of starting are to look at factors affecting confidentiality, integrity and availability and build it around that, or perhaps brainstorming is the preferred starting point?

References

Collette, R. (2006). Overcoming obstacles to data classification [information security]. *Computer Economics Report (International Edition), 28*(4), 8-11.

Fibikova, L., & Müller, R. (2011). A Simplified Approach for Classifying Applications. In N. R. Pohlmann, Helmut; Schneider, Wolfgang (Ed.), *ISSE 2010 Securing Electronic Business Processes* (pp. 39-49): Vieweg+Teubner.

Ghernaouti-Helie, S., Simms, D., & Tashi, I. (2011). *Protecting Information in a Connected World: A Question of Security and of Confidence in Security*. Paper presented at the 14th International Conference on Network-Based Information Systems (NBiS).

Glynn, S. (2011). Getting To Grips With Data Classification. *Database and Network Journal,*

41(1), 8-9.

Hayes, J. (2008). Have data will travel - [IT security]. *Engineering & Technology*, *3*(15), 60-61.

Kane, G., & Koppel, L. (2013). Chapter 1 - Information Protection Function One: Governance. In G. K. Kane, Lorna (Ed.), *Information Security* (pp. 1-11). Boston: Elsevier.

Oscarson, P., & Karlsson, F. (2009). *A National Model for Information Classification*. Paper presented at the AIS SIGSEC Workshop on Information Security & Privacy (WISP2009), Phoenix, AZ, USA.

Swedish Civil Contingencies Agency. (2014). En bild av myndigheternas informationssäkerhetsarbete 2014 – tillämpning av MSB:s föreskrifter [A picture of governmental agencies work with information security 2014 - application of the Swedish Civil Contingencies Agency guidelines] (Vol. MSB740): Swedish Civil Contingencies Agency,.