An emergent dynamic risk-based information classification process

Martin Lundgren, Luleå Technical University & Erik Bergström, University of Skövde

In the past decade, much research and standards have focused on developing various approaches to mitigate IS risks in order to create relevant and effective Information Security Management Systems (ISMS) (Bowen et al. 2006; ISO/IEC 2013; NIST 800-37 2010). Risk Analysis (RA) is the common term and field to balance the value of information assets for protection against identified risks and a prerequisite for selecting possible security measures to mitigate those risks to an acceptable level (Eloff et al. 1993; Fowler 2003; Gerber and Solms 2005). A central part of RA is Information Classification (IC), that identify organizational assets and decides what consequences a loss of confidentiality, integrity, or availability could cause (Breier and Schindler 2014; Fowler 2003). The literature often depicts IC and RA as an isolated sequential process performed in a linear progression: where IC serves as input for the RA that leads to a rational decision in regard to implemented security measures (ISO/IEC 2013; Reed 2007; Straub and Welke 1998). IC is thus a critical part of RA, as it is what enables adequate security measures to be recognized, whilst inadequate identification or valuation of assets may misguide such decisions (Shedden et al. 2010; von Solms and von Solms 2004).

Although critical for ISMS, it remains unclear how IC and RA interoperate in relation to recognized security measures. For example, how and what information to classify before the RA is not always evident (Ozkan and Karabacak 2010) and it has been described as one of the main difficulties in assessing RA (Sajko et al. 2006). Nor is the interplay between IC, RA and security measures evident while adapting to new configurations, or what constitutes as adequate security measures with respect to IC and RA (Baskerville 1991; Taylor 2015). Yet much research does not deliberate these challenges (Sajko et al. 2006; Tatar and Karabacak 2012), but address them as self-evident (Farahmand et al. 2005; Moulton and Moulton 1996). We argue however that IC, RA and resulting security measures should not be seen as a sequential process, but as an emergent dynamic process where IC, RA and security measures interoperate with respect to new configurations (Kim and Lee 2005).

A literature study in the IS basket journals on capabilities and challenges with IC and RA have been performed. The preliminary results show that similar capabilities and challenges exist in the respective areas and these results have been used to construct an interview guide aimed at exploring the current gap between IC, RA and security measures. A number of Swedish government agencies have been selected to be interviewed based on a previous study by Bergström et al. (2016), where the government agencies submitted their internal policies or guidelines for review. The preliminary results indicate there are several interesting approaches used in Swedish government agencies that challenge the current view. The overall aim is to investigate these gaps, clarify what is needed in the transitions between IC, RA and security measures, what triggers change or transitions between them and connect them to the life-cycle perspective present in an ISMS.

References

Baskerville, R. 1991. “Risk analysis: an interpretive feasibility tool in justifying information systems security,” *European Journal of Information Systems,* (1:2), pp. 121–130.

Bergström, E., Åhlfeldt, R.-M., and Anteryd, F. 2016. *Informationsklassificering och säkerhetsåtgärder*.

Bowen, P., Hash, J., and Wilson, M. 2006. “Information security handbook :: a guide for managers,” No. NIST SP 800-100, , Gaithersburg, MD: National Institute of Standards and Technology (available at http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-100.pdf).

Breier, J., and Schindler, F. 2014. “Assets Dependencies Model in Information Security Risk Management,” in *Information and Communication Technology*, Linawati, M. S. Mahendra, E. J. Neuhold, A. M. Tjoa, and I. You (eds.), (Vol. 8407), Berlin, Heidelberg: Springer Berlin

Heidelberg, pp. 405–412 (available at http://link.springer.com/10.1007/978-3-642-55032-4_40).

Eloff, J. H. P., Labuschagne, L., and Badenhorst, K. P. 1993. “A comparative framework for risk analysis methods,” *Computers & Security*, (12:6), pp. 597–603 (doi: 10.1016/0167-4048(93)90056-B).

Farahmand, F., Navathe, S. B., Sharp, G. P., and Enslow, P. H. 2005. “A Management Perspective on Risk of Security Threats to Information Systems,” *Information Technology and Management*, (6:2–3), pp. 203–225 (doi: 10.1007/s10799-005-5880-5).

Fowler, S. 2003. “Information Classification–Who, Why and How?,” *GIAC Sescurity Essentials Certification (GSEC)*, (1).

Gerber, M., and Solms, R. von. 2005. “Management of risk in the information age,” *Computers & Security*, (24:1), pp. 16–30 (doi: https://doi.org/10.1016/j.cose.2004.11.002).

ISO/IEC, 27001. 2013. *ISO/IEC 27001: Information technology-Security techniques -Information security management systems - Requirements*, ISO.

Kim, T., and Lee, S. 2005. “Design Procedure of IT Systems Security Countermeasures,” in *Computational Science and Its Applications – ICCSA 2005*, O. Gervasi, M. L. Gavrilova, V. Kumar, A. Laganà, H. P. Lee, Y. Mun, D. Taniar, and C. J. K. Tan (eds.), (Vol. 3481), Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 468–473 (available at http://link.springer.com/10.1007/11424826_49).

Moulton, R. T., and Moulton, M. E. 1996. “Electronic communications risk management: A checklist for business managers,” *Computers & Security*, (15:5), pp. 377–386 (doi: 10.1016/0167-4048(96)82560-0).

NIST 800-37. 2010. “Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach.,”

Ozkan, S., and Karabacak, B. 2010. “Collaborative risk method for information security management practices: A case context within Turkey,” *International Journal of Information Management*, (30:6), pp. 567–572.

Reed, B. 2007. “Implementing Information Lifecycle Security (ILS)*,” *Information Systems Security*, (16:3), pp. 177–181 (doi: 10.1080/10658980601144907).

Sajko, M., Rabuzin, K., and Bača, M. 2006. “How to calculate information value for effective security risk assessment,” *Journal of Information and Organizational Sciences*, (30:2), pp. 263–278.

Shedden, P., Smith, W., and Ahmad, A. 2010. “Information security risk assessment: towards a business practice perspective.,”

von Solms, B., and von Solms, R. 2004. “The 10 deadly sins of information security management,” *Computers & Security*, (23:5), pp. 371–376 (doi: 10.1016/j.cose.2004.05.002).

Straub, D. W., and Welke, R. J. 1998. “Coping with Systems Risk: Security Planning Models for Management Decision Making,” *MIS Quarterly*, (22:4), p. 441 (doi: 10.2307/249551).

Tatar, Ü., and Karabacak, B. 2012. “An hierarchical asset valuation method for information security risk analysis,” in *International Conference on Information Society (i-Society 2012)*, , June, pp. 286–291.

Taylor, R. G. 2015. “Potential Problems with Information Security Risk Assessments,” *Information Security Journal: A Global Perspective*, (24:4–6), pp. 177–184 (doi: 10.1080/19393555.2015.1092620).