Chapter 63
Genre-Based Approach to Assessing Information and Knowledge Security Risks

Ali Mohammad Padyab
Luleå University of Technology, Sweden

Tero Päivärinta
Luleå University of Technology, Sweden

Dan Harnesk
Luleå University of Technology, Sweden

ABSTRACT

Contemporary methods for assessing information security risks have adopted mainly technical views on information and technology assets. Organizational dynamics of information management and knowledge sharing have gained less attention. This article outlines a new, genre-based, approach to information security risk assessment in order to orientate toward organization- and knowledge-centric identification and analysis of security risks. In order to operationalize the genre-based approach, we suggest the use of a genre-based analytical method for identifying organizational communication patterns through which organizational knowledge is shared. The genre-based method is then complemented with tasks and techniques from a textbook risk assessment method (OCTAVE Allegro). We discuss the initial experiences of three experienced information security professionals who tested the method. The article concludes with implications of the genre-based approach to analyzing information and knowledge security risks for future research and practice.

INTRODUCTION

More than a decade ago, Dhillon and Backhouse (2000) highlighted the importance of understanding and protecting information assets instead of merely focusing on physical and technical assets in the field of information security. Indeed, many if not most current risk assessment methods base their analysis on the concept of "information assets" (Jones & Ashenden, 2005). However, a few researchers have criticized current risk assessment methods by illustrating some deficiencies in the

DOI: 10.4018/978-1-4666-8473-7.ch063

asset identification task. Methods may define what an information asset is, but they seem to assume that the risk analyst will then simply know the organization's information assets without further assistance for identification (Campbell & Stamp, 2004).

Moreover, most risk analysis methods are regarded as providing a simple technical view on information (data) and technological assets, ignoring the dynamic environment of knowledge work and people as knowledgeable entities of the organization (Shedden, Smith, & Ahmad, 2010; Spears, 2006). For example, a recent case study (Shedden, Scheepers, Smith, & Ahmad, 2011) suggests that a relatively well-known risk analysis method (OCTAVE-S) fails to address knowledge security issues related to informal and non-technical organizational processes.

We started to address this knowledge gap with the assumption that knowledge security may be at risk in situations where knowledge is shared between people and organizations. Knowledge sharing may concern both tacit and explicit knowledge, and it involves the knowledge creation modes of externalization, socialization, combination, and internalization (Nonaka, 1994). All of these modes of knowledge creation and sharing require communication between people, either directly through human-to-human knowledge networks or through externalized information repositories (Alavi & Leidner, 2001; Nonaka, 1994).

Hence, we looked at theories and concepts which would help us to conceptualize organizational communication patterns as a basis for mapping security risks related to knowledge sharing. Among such theories, the genre theory of organizational communication (Yates & Orlikowski, 1992) provided us with a well-established conceptual basis, as well as established analytical means, with regard to both human-to-human communication such as meetings (Antunes & Costa, 2003; Orlikowski & Yates, 1994) and documented information (Karjalainen, Päivärinta, Tyrväinen, & Rajala, 2000). Hence, we employed an already-established Genre-Based Method (GBM) (Päivärinta, Halttunen, & Tyrväinen, 2001) to identify and analyze organizational knowledge-sharing communications.

We then combined GBM with a lightweight risk assessment method, OCTAVE Allegro (OA) (Caralli, Stevens, Young, & Wilson, 2007) to relate risk assessment to the genre-based model of organizational knowledge. With the objective of evaluating the resulting hybrid method (GBM-OA), we introduced it as part of an online master's course on knowledge security. Three experienced information security professionals, who were asked to try out the method and make a security risk analysis in their own organizations, attended the course. Their feedback on the method in practice provided us with insight and ideas for improvement. Here we report on the hybrid method of GBM-OA and its initial evaluation in the aforementioned setting.

We will first present the theoretical background and introduce the GBM-OA method. This is followed by the reflections of the three professionals who tested it in their companies. We discuss the contributions and implications of the genre-based approach in security risk assessment. Finally, we indicate limitations and ideas for further research.

BACKGROUND

Security Risk Assessment

Risk assessment seeks to "identify, measure, quantify and evaluate risks and their consequences and impacts" (Haimes, 2004, pp. 22). The output of risk assessment helps organizations conduct cost-benefit analyses based on current controls and countermeasures that analyze whether to mitigate, transfer, avoid, or accept the risks (Baskerville, 1993; Haimes, 2001; Peltier, 2005). Today there are more than 200 practitioner-oriented risk assessment methods and other academic security models available (Dubois, Heymans, Mayer, &