Chapter 20
A Multi-Level Relational Risk Assessment Model for Secure E-Government Projects

Dionysis Kefallinos
National Technical University of Athens, Greece

Maria A. Lambrou
University of the Aegean Business School, Greece

Efstathios D. Sykas
National Technical University of Athens, Greece

ABSTRACT

In this chapter, the authors propose a model for a risk assessment tool directed towards and tailored specifically for e-government projects. The authors' goal is to cover the particular threats pertinent to the e-government project context and provide an interface between the broader philosophy of IT governance frameworks and the technical risk assessment methodologies, thus aiding in the successful and secure implementation and operation of e-government infrastructures. The model incorporates a wide range of applicable risk areas, grouped into eleven levels, as well as seven accompanying dimensions, assembled into a checklist-like matrix, along with an application algorithm and associated indices, which an evaluator can use to calculate risk for one or for multiple interacting projects.

INTRODUCTION

In this chapter we propose a risk assessment (RA) method and tool directed towards and tailored specifically for e-government projects. Given the diversity of concepts in e-government, creating a workable definition is becoming increasingly difficult (Roy, 2003). Generally, e-government refers to strategies, organizational forms and processes, as well as information technology employed so as to enhance access to and delivery of government information and services to citizens, businesses, government employees and other agencies. From a technical standpoint, e-government initiatives usually involve several types of digital technology and information systems, including databases,

DOI: 10.4018/978-1-4666-1740-7.ch020

networking, collaboration services, multimedia, tracking and tracing, and and privacy technologies (Snellen, 2002). In particular, we consider e-government projects as technical ventures that further the cause of modeling and transfer of G2G, G2B and G2C processes into the electronic world; they typically include and deal with (both in their development as well as their operational phase) public servants, private enterprises, professionals and the general public.

The important issues and impediments for the successful design, deployment and use of secure e-government (and in general e-service) infrastructures have been documented extensively (Curthoys & Crabtree, 2003; Gil-Garcia & Pardo, 2005; Jaeger, 2003; Löfstedt, 2005; Martin, 2005; Relyea, 2002; Vassilakis, Lepouras, Fraser, & Georgiadis, 2005), depicting the range of highly complex and diverse challenges public managers and security professionals must face in the their design, implementation and operation. It is generally accepted that success is less about selecting the right technology and more about managing organizational capabilities, facing regulatory constraints and environmental pressures and anticipating social, political and psychological issues of people involved; in other words effectively assessing risks and governing technological structures, within context.

Efficient management and security of a complex information and communications technology (ICT) system essentially depends on concise specification of requirements and security goals, their correct and consistent transformation into policies and appropriate deployment, enforcement and monitoring of these policies. This has to be followed-on by an incessant process to adapt the policies to changing contexts, environments, technologies, usage patterns and attack methods. To help understand the complex interrelations between security policies and ICT infrastructure and vulnerabilities, to validate security goals and especially to raise the assurance level of the RA process and the confidence level to the reviewed system, formal tool-based methodologies are necessary, which, as an additional benefit, also guide towards a systematic evaluation and assist in determining exactly what really needs protection and which security policies to apply.

The RA tool that we model in this chapter can be viewed as an extension of established technical ICT RA approaches, aiming to: (i) better target the security and privacy goals in e-government projects, since a contextualized tool promotes improved formulation and facilitation of accurate security-related decisions, (ii) form a connection between technical ICT RA methodologies and Information Technology Governance (ITG) frameworks, (iii) increase security and privacy awareness by promoting the active involvement of a larger variety of non-technical personnel, and finally (iv) facilitate the application of baseline security and privacy policies.

Our motivation for the development of the presented model stems from experiences and observations in the RA field, whereupon a lack of adequate interaction between the technical methodologies (as well technology oriented practitioners and researchers) and the managerial ones has been clearly evident, especially in a context where public servants, the private industry and the general public interact with each other. Therein, a number of problematic aspects are witnessed in the development, implementation and production phases, precisely because of this "disregard", the result being a downgrade of the importance, confidence and acceptance of the results and suggestions of RA, which are often too narrow in scope anyway.

In section 2 of the chapter, a brief overview of the concepts and the background of our model is given, the techniques, standards, tools and practices upon which it is based, including general-purpose and ICT RA methodologies and tools, as well as ITG frameworks. We follow that with a detailed description of our model in section 3, and a discussion on its usage and our surmises