Chapter 19
Raising Information Security Awareness in the Field of Urban and Regional Planning

Margit Christa Scholl
Technische Hochschule Wildau, Wildau, Germany

ABSTRACT

IT is being increasingly used in most areas of life. With the IoT, this technology is set to be in a state of continuous evolution in urban and regional settings. The ongoing development of digitalization processes also increases the possibilities of abuse—both at the technical and interpersonal level. Better information security (IS) awareness (ISA) and knowledge about the dangers that accompany digitalization and the corresponding protective measures are important in private and work life. However, ISA is often overlooked. Training the relevant awareness and skills should also be included in urban and regional planning for citizens. This article thus provides a review of the scientific literature of leading academic journals in the area of IS and the transfer of scientific knowledge for practical purposes. The article presents Serious Games as a way to achieve a deeper understanding of how to promote sustainable ISA using creative methods. Furthermore, ideas of how to apply the Fun Theory and its practice to integrate awareness into modern urban and regional planning will be discussed.

1. INTRODUCTION

Nowadays, we increasingly depend on information technology (IT) in our work and private lives. In the modern information society, computers and computer networks are becoming more and more important to business processes and for performing specialized tasks. IT transmits, electronically processes, and stores large amounts of data and a wide variety of information (BAköV, 2009). However, previous IT security mechanisms have reached their limits, and reliability and controllability cannot be assumed as the norm (BSI 2015). Government digital agendas—such as that of the Federal Government of Germany[1] or the European Digital Agenda[2]—seek to keep abreast of digital networking and the digital changes in society.

DOI: 10.4018/978-1-6684-3698-1.ch019

However, at the same time cybersecurity is creating new challenges. The term information security, as used in (inter)national standards, consists of more than just IT security. The goal of information security (IS) is to protect information of all types and origins (BAköV, 2009). Risk management in cyberspace must become part of national efforts. In this sense, all cities and regions face major challenges in terms of promoting digitalization on the one hand and responsibility towards their citizens on the other.

Digitalization is a core aspect of the "smartness" of the Internet of Things (IoT), smart homes, smart grids, and the smart city. Nevertheless, as summarized in Scholl and Scholl (2014), a smart city as an urban space would have the characteristics of a culture of innovation, a high quality of life—also referred to as "liveability"—global competiveness and attractiveness, security and safety, and economic and environmental sustainability. A smart city would have a smart municipal government managing and implementing policies towards those ends by leveraging ICT and institutions and by actively involving and collaborating with stakeholders (Al Awadhi et al., 2012). As the current *CIP Report* points out, smart-city projects are increasingly dominating the conversation around the future of urban environments and have also introduced a range of security challenges (Gordon & McAleese, 2017). To achieve trust in the development of smart cities, IS must be an integral part of the initiatives. Because both individuals and organizations are affected by IS challenges and information security awareness (ISA), these trainings (ISAT) should be provided for everyone on an ongoing daily basis. Von Solms and von Solms (2018) are working on simplifying the terminology to be used in the governance of cybersecurity and IS in order to explain to the boards of directors and executive management their responsibilities and accountability in this regard.

The results of a survey conducted in 2014 among EU and German citizens show that about 33 per cent of those questioned said that they were very concerned about becoming victims of identity theft.[3] To overcome this, values like integrity, honesty, and trust are required at the individual level, as well as professional and business competency accompanied by management and leadership skills: these include maintaining a positive attitude, team building, empowerment, coaching and training others, and influencing decision makers to embrace new standards of achievement and social behaviour that lead to appropriate IS and organizational resilience (Sullivant, 2016). Once damage has occurred to businesses, public administrations, and governmental or other institutions (see figure 1), it can trigger a chain of events with adverse effects for smart cities and electronic government (e-government) or future smart government.

But what does this mean for urban and regional planning processes in more concrete terms? In the opinion of the author, responsibility for the ISA of employees falls not only to companies but also to cities and municipalities, which should provide education for their inhabitants. This means establishing a general programme to provide information about threats and risks, vulnerabilities (which are gaps in the security of a system or a software or in the organization itself), the various kinds of attacks, and possible damage: this programme should be implemented creatively through urban and regional planning (see Figure 1). Moreover, the cybersecurity authorities and intelligence services around the world would, in principle, have to cooperate with one another to track down perpetrators. The demand coming from authorities and companies for comprehensive digitalization must go hand in hand with IS—which in turn must be accompanied by awareness. ISA affects everyone in society.

The research questions in this paper are:

RQ #1: What are the main current scientific findings from the field of occupational ISA and ISAT that can be used in practice?