Chapter 42
Metrics for Ensuring Security and Privacy of Information Sharing Platforms for Improved City Resilience: A Review Approach

Jaziar Radianti
Centre for Integrated Emergency Management UiA, Grimstad, Norway

Terje Gjøsæter
Oslo Metropolitan University, Oslo, Norway

ABSTRACT

City resilience is a pressing issue worldwide since the majority of the population resides in urban areas. When disaster strikes, the consequences will be more severe in the cities. To achieve resilience, different organizations, agencies and the public should share information during a disaster. ICT-based community engagement is used for strengthening resilience. The authors propose a set of metrics for assessing the security and privacy of information sharing tools for resilience. They then apply the selected metrics to a selection of information sharing tools. The authors' main finding is that most of them are reasonably well-protected, but with less than private default settings. They discuss the importance of security and privacy for different important categories of users of such systems, to better understand how these aspects affect the willingness to share information. Security and privacy is of particular importance for whistle-blowers that may carry urgent information, while volunteers and active helpers are less affected by the level of security and privacy.

DOI: 10.4018/978-1-7998-8954-0.ch042

1. INTRODUCTION

The UNDESA projection shows that the proportion of the world's population living in urban areas will increase from 54% (2014) to 66% by 2050 (UN, 2014). Thus, it is evident why city resilience has been emphasized globally due to cities becoming more vulnerable as more people will be affected when unexpected events occur. Information sharing is an important way to enhance resilience in a disaster (Palen et al., 2010; Yang & Maxwell, 2011), with the help of information and communication technology (ICT) tools that are becoming acceptable for facilitating crisis communication (Pipek, Liu, & Kerne, 2014). Interpreting further the spirit of the Hyogo Framework Action (UNISDR, 2005), the overall capability to cope with hazards is not solely authority responsibility, but is a combination of the self-organizing capability of the individuals, communities, public and private organizations in affected areas. Furthermore, the Sendai Framework for Disaster Risk Reduction 2015-2030 outlines the importance of building resilience into policies, plans and programmes. Sendai Framework encourages the use of information and communications technology to enhance measurement tools and the collection, analysis and dissemination of data, as well as to collaborate with people at the local level through the involvement of both community-based and non-governmental organizations.

In brief, the role of ICT tools to enable the society in general to adapt and recover from hazards and stresses is evident (Trnka & Johansson, 2011), especially to ensure that the right information flows smoothly to the intended audience.

What is resilience? UNISDR (2004) defines resilience as "the capacity of a system, community or society potentially exposed to hazards to adapt, by resisting or changing in order to reach and maintain an acceptable level of functioning and structure". We adopt this definition, and suggest that resilience should include the ability of individuals and communities to absorb and prepare to make use of the different crisis management communication technologies, so that they can engage and share information better with each other and with public authorities. The definition should also include the capacity for learning practical security and privacy knowledge for better use of ICT-based engagement tools.

The recent trend of ubiquitous computing allows people to share information by using day-to-day technologies surrounding them. The presence of social media in combination with the powerful trend of crowdsourcing for obtaining data shared by citizens (Liu, 2014; Liza, 2011), has to some extent been accepted as a part of crisis communication, apart from the data quality weaknesses that may arise from social media information (Tapia & Moore, 2014). Sharing information using various means arguably improves resilience as individuals can contribute information faster to the authorities, as well as to the circle of family and friends they care about and improve the way responders manage the crisis (Lindsay, 2011; Trnka & Johansson, 2011).

However, the crucial questions that should be addressed are: how thoroughly are the privacy and security concerns considered in line with the encouragement of the information sharing among different components of a resilient society? Does information sharing increase the resilience, or could it in some situations weaken the resilience when a focus on security and privacy emerge?

Information security concerns protecting information in different contexts: its confidentiality, integrity and availability (Avižienis, Laprie, Randell, & Landwehr, 2004). Security of information is essential to some organizations and actors before they are willing to share it (Liu & Chetal, 2005). For private citizens, trust concerning privacy protection is crucial, covering personal sensitive information (PSI) and personally identifiable information (PII, information that can identify them) (Schwartz & Solove, 2011). Part of the resilience is that our information is verifiably unmodified, confidential, available when