

Telework and Data Privacy and Security

Reima Suomi

Turku School of Economics, Finland



INTRODUCTION

Telework is a major phenomenon of the information society. It refers to work being done independently of time and place, still often in an employment relationship with an organization, and heavily supported by modern information and communication technology. Telework can also be identified in terms such as e-work and distance work or telecommuting, in general telework is a part of the virtual organization metaphor. Telework, through its liberty from place and time specificity or performing work, is a major change agent leading us towards a new information and knowledge society. It is expected to bring in productivity, better output quality and employee, employer and customer satisfaction. A better utilization of human resources can be expected, as through telework employees can work to many organizations, so sharing and also strengthening their professional skills and status.

Yet telework is not spreading as fast in the society as one could expect. One reason can be seen in data privacy and security discussion. Almost any telecommunication application can be undermined through strong arguments about missing data privacy and security. Many telework arrangements have also fallen into this trap. While privacy and security surely are values to be maintained, a possible violation of them should not be used as an excuse to undermine a value-adding application of modern information technology.

This chapter discusses the needs for data security and privacy in telework, and delivers a framework on the most threatening risks on the security and privacy in teleworking environments. A goal is to try to find out, whether telework really is a data security risk for organizations, or whether the threats have been exaggerated.

Telework can be defined as follows (Suomi & Pekkola, 1998, p. 221): *Telework is a working arrangement where at least some parts of the working tasks are performed outside the regular working place in an employee-employer -relation, and where information technology is an important tool.* The term telework

is more usual in Europe, whereas Americans prefer to talk of telecommuting (Jacobs & Van Sell, 1996; Steve, 1996) More recently the term “eWork” in many variations (e-Work, E-work, eWorking) has become more fashionable (Davenport, Thomas, & Cantrell, 2002). In general, telework discussion can be seen as a subtopic of the discussion on virtual organizations (Markus, Manville, & Agres, 2000).

Telework is a phenomenon changing the society in a wide range of issues. Among the issues surrounding debate of telework we can mention the following:

- Telework is a part of a wider change process in working and organizational cultures leading from the industrial society towards the information society
- Production of goods and services will be distributed through binding together geographically distant production entities and through introducing new partners into established production entities in a way that benefits all—simultaneously possibilities for telework emerge
- An important part of the process is more intensive use of modern information and communications technology
- Organizational cultures turn into cooperation-seeking and customer-oriented ones
- Continuous education for the work-force (lifelong learning) plays a paramount role
- Organization of work is based on flexible job categories and contents.

During the last few years, viruses and spam mail have become number one headaches for many chief information officers. Almost any information system implementation—especially telecommunication dependent—can be undermined through strong arguments about missing data privacy and security. We have several examples of areas where data privacy and security concerns have hindered the development of information systems. Health care in general is a very sensitive area to data privacy and security, and fears in relation to these have

slowed down many developments (Johnson-Page & Thatcher, 2001; Rindfleisch, 1997; Van der Haak et al., 2003). In banking and money transfer, security is of course a major issue, on which a lot has been invested (Davies & Price, 1984). Electronic commerce is a major example of an information system's application area where privacy concerns have clearly inhibited the development of business (Hoffman, Novack, & Peralta, 1998; Wang, Lee, & Wang, 1998).

In this chapter the research question is, "Which are the risks of secure and private telecommunication in teleworking environments?"

In addition to the theory-building phase, the motivations to build data security and privacy rules are questioned. Here the research questions are: Is the need for privacy and security often exaggerated in telework arrangements? and Which are the outcomes of giving security and privacy too much emphasis in telework practice?

The chapter unfolds as follows: in the section 2 we build a framework of the telework IT-infrastructure. This allows us to understand the telework situation. In the next section, we discuss some of the most visible risks towards data security and privacy in this environment. Finally, in section 4 conclusions are drawn.

A FRAMEWORK ON DATA SECURITY AND PRIVACY ISSUES IN TELEWORK

Our key terms are defined as follows:

Data Security

Data files are not subject to unauthorized access, change or destruction (adapted from (Laudon & Laudon, 1998)).

Data Privacy

Right of an individual to participate in decisions regarding the collection, use, and disclosure of information personally identifiable to that individual (adapted from (Alter, 1997)).

Data security is valuable as such, but is too an absolute condition for data privacy. Without data security data privacy is impossible to implement.

Telework introduces two major threats to data security:

1. Through telework work is dispersed to a geographically wide area. Work happens in various places, and so data and devices carrying it is also often disseminated. This makes access control very difficult.
2. For teleworkers, access from outside to the centralized information processing resources must be catered for. This same gateway can be used by other external and harmful intruders too, and in addition the extra telecommunication needed is a security threat by itself.

A much discussed topic is that of doing telework at home. Home, by development, is an open environment for the family members, and access controls are difficult to implement in practice. A room or a computer is often shared between the family members. Work and home roles intermix, and data security can be severely threatened.

In the rest of the chapter we will discuss the second issue in some more detail, as it is connected more to information systems and network technology than the first issue. Figure 1 presents a basic conceptual framework on telework infrastructure that we can then use in our later analysis of threats towards data security and privacy.

In the framework we see the host organization domain referring to the part of telework IT-infrastructure that is administered through the host organization. In addition to this, we have the Teleworker administered domain, which usually is the same thing as his or her computer or computer network at home. By 'administered,' we refer to the activities of:

- 1 Maintaining virus protection
- 2 Filtering spam mail
- 3 Keeping up firewalls
- 4 Maintaining software

In the teleworker administered domain, we see the work area and other areas. These other areas might be connected to leisure or to work with other host organizations. These areas might use shared resources as it comes to databases, telecommunication lines, computer resources, as well as to physical office base and all the other resources contained in it.

In the framework we also see two databases. One is at the host organization domain, and another is at the teleworker domain. Here, the database should be

3 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/telework-data-privacy-security/17801

Related Content

Augmented Reality Indoor Navigation Using Handheld Devices

Angelin Gladstonand Aadharshika Duraisamy (2019). *International Journal of Virtual and Augmented Reality* (pp. 1-17).

www.irma-international.org/article/augmented-reality-indoor-navigation-using-handheld-devices/228943

Augmented Reality Indoor Navigation Using Handheld Devices

Angelin Gladstonand Aadharshika Duraisamy (2019). *International Journal of Virtual and Augmented Reality* (pp. 1-17).

www.irma-international.org/article/augmented-reality-indoor-navigation-using-handheld-devices/228943

Methods for the Measurement and Visualization of Social Networks in Multi-User Virtual Worlds

Devan Rosen (2011). *Handbook of Research on Methods and Techniques for Studying Virtual Communities: Paradigms and Phenomena* (pp. 530-541).

www.irma-international.org/chapter/methods-measurement-visualization-social-networks/50361

Sustainable E-Learning Communities

Chris Stary (2009). *Virtual Community Practices and Social Interactive Media: Technology Lifecycle and Workflow Analysis* (pp. 400-413).

www.irma-international.org/chapter/sustainable-learning-communities/30828

Building Trust in Virtual Communities

István Mezgar (2008). *Virtual Technologies: Concepts, Methodologies, Tools, and Applications* (pp. 35-43).

www.irma-international.org/chapter/building-trust-virtual-communities/30909