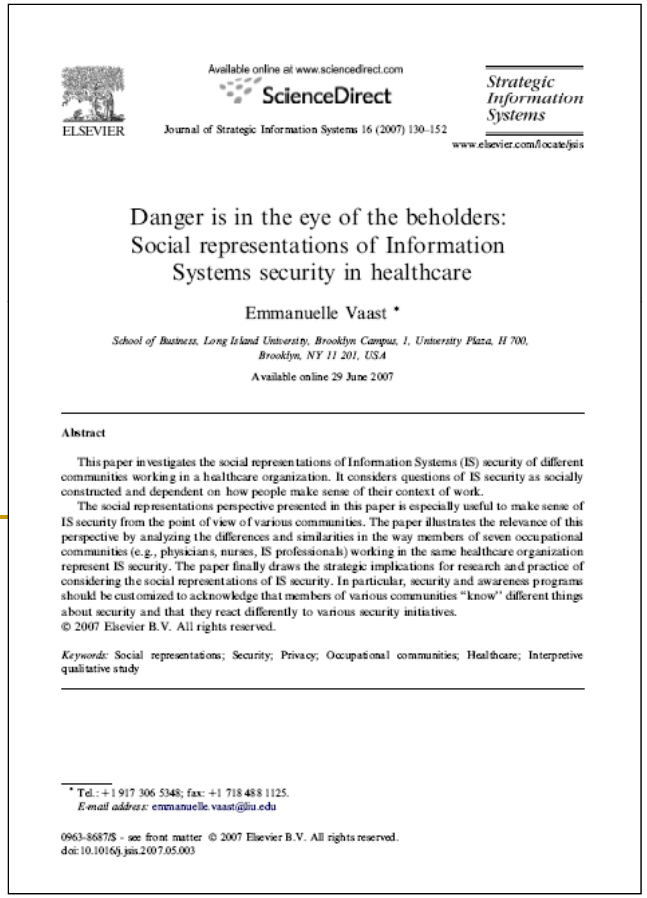
Danger is in the eye of the beholders: Social representations of Information Systems security in healthcare

Emmanuelle Vaast,

School of Business, Long Island University, Brooklyn Campus, 1, University Plaza, H 700,

Brooklyn, NY



Available online at www.sciencedirect.com
ScienceDirect
Journal of Strategic Information Systems 16 (2007) 130–152
Strategic Information Systems
ELSEVIER
www.elsevier.com/locate/jsis

Danger is in the eye of the beholders: Social representations of Information Systems security in healthcare

Emmanuelle Vaast *

School of Business, Long Island University, Brooklyn Campus, 1, University Plaza, H 700, Brooklyn, NY 11 201, USA

Available online 29 June 2007

Abstract

This paper investigates the social representations of Information Systems (IS) security of different communities working in a healthcare organization. It considers questions of IS security as socially constructed and dependent on how people make sense of their context of work.

The social representations perspective presented in this paper is especially useful to make sense of IS security from the point of view of various communities. The paper illustrates the relevance of this perspective by analyzing the differences and similarities in the way members of seven occupational communities (e.g., physicians, nurses, IS professionals) working in the same healthcare organization represent IS security. The paper finally draws the strategic implications for research and practice of considering the social representations of IS security. In particular, security and awareness programs should be customized to acknowledge that members of various communities "know" different things about security and that they react differently to various security initiatives.

© 2007 Elsevier B.V. All rights reserved.

Keywords: Social representations; Security; Privacy; Occupational communities; Healthcare; Interpretive qualitative study

* Tel.: +1 917 306 5348; fax: +1 718 488 1125.
E-mail address: emmanuelle.vaast@liu.edu

0963-8687/$ - see front matter © 2007 Elsevier B.V. All rights reserved.
doi:10.1016/j.jsis.2007.05.003

Purpose of Paper

- Investigates social representations of IS in healthcare.
- Consider questions of IS security as socially constructed.

Social Representations Perspective

- Social Representations Perspective …
  - are Socio-cognitive
  - assumes social representations and practices are related to each other and mutually influence each other over time
  - act as sensitizing concepts
  - are Polyphasic
  - are not static

Occupational communities	Job	Access to IS	Interactions with
IS professionals	Manage Information Systems. Provide equipments and update systems. Make sure no disruption of system is experienced	Personal workstation Access to: internet, intranet, office tools, administrator's rights on network	Managers and peers mostly
Physicians	Clinicians in charge of medical care of inpatients and outpatients. Consultation, prescriptions, surgery, and follow-ups of patients	Shared workstation on wards Access to: internet, intranet, office tools, some medical systems (lab results)	Patients, nurses, clerks, and peers mostly Managers and technicians to a lesser extent
Nurses	Clinicians who assist physicians in the physiological care of patients. Medications, regular check of patients' reactions to provided care	Shared workstation on wards Access to: internet, intranet, office tools, some medical systems (lab results, analysis and medication orders)	Patients and peers mostly, also physicians and clerks Managers and technicians to a lesser extent
Social workers	Provide socio-psychological support to patients. Follow up of inpatients and outpatients in critical psycho-sociological situations	Personal workstation Access to: internet, intranet, office tools	Patients and peers mostly, also nurses, clerks, and physicians
Clerks	Liaison between administrative functions and medical personnel. Registration and release of patients, communications with health insurance companies	Shared workstation on wards Access to: internet, intranet, office tools, some medical systems (lab results, analysis and medication orders), administrative systems (billing, release)	Physicians, nurses, managers, and peers mostly, sometimes patients and physicians as well
Technicians	Manipulate medical equipment. Maintain all technical equipment (machines, operations rooms, etc.)	Shared workstation on wards Access to: internet, intranet, office tools, some medical systems (entry of lab results), for some	Nurses and peers mostly, sometimes physicians, managers, and patients
Managers	Supervise the different services and departments. Deal with the administrative functions and manage the human and financial resources of Eastern Hospital	Personal workstation Access to: internet, intranet, office tools, administrative systems	IS professionals, clerks, nurses, peers, and physicians, mostly

Employee Age and Yrs at Hospital

Summary of respondents at Eastern Hospital

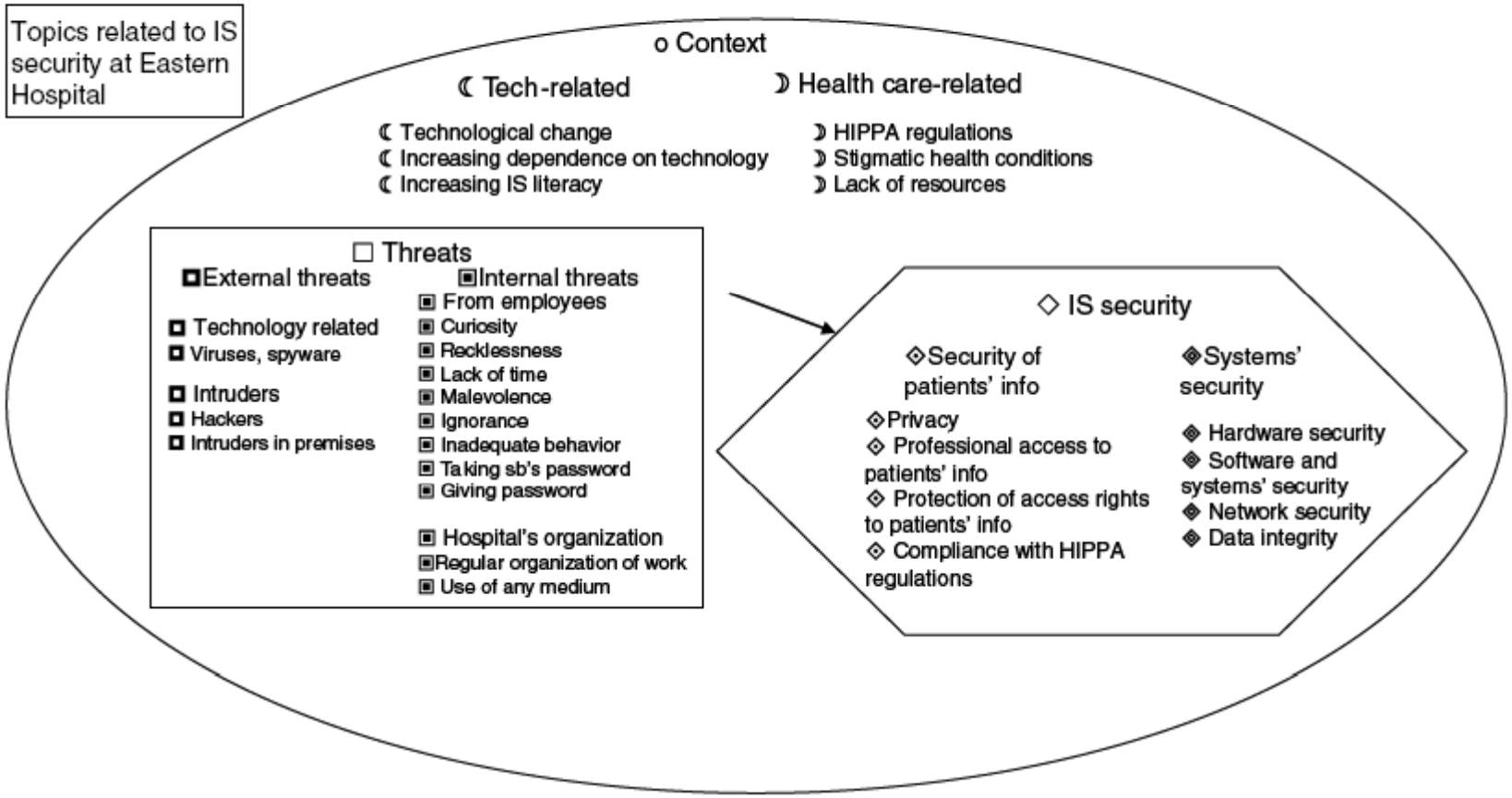
Gender	Clerks	IS professionals	Managers	Nurses	Physicians	Social workers	Technicians	Total
Occupational communities								
Female	6	1	5	6	2	6	2	28
Male		5	1		3		2	11
Total	6	6	6	6	5	6	4	39

	Yrs in Profession	Number of respondents		Yrs at Eastern Hospital	Number of respondents
	<5 yrs	5		<5 yrs	9
	5–9 yrs	8		5–9 yrs	14
	10–14 yrs	3		10–14 yrs	2
	15–19 yrs	10		15–19 yrs	7
	>20 yrs	13		>20 yrs	7
	Total	39		Total	39

Interview Focus

1. background information on respondent's job and situation
2. respondent's use of IS
3. definition of IS security
4. threats to IS security
5. management of IS security
6. peers and future perspectives on IS security
7. anecdote or critical incident related to IS security

Categories From Respondents' Disclosure



Mean frequency of occurrence of topics defining IS security

Mean frequency of occurrence of topics defining IS security

Occupational communities	Privacy of Patients' information	Professional access to patients' information	Respect of access rights to patients' information	Compliance with HIPAA regulations	Total IS Security as security of patients' information	Total IS Security as Systems' Security (hardware, software, network, and data integrity)
Definition of IS security						
IS professionals	0.50	0.00	0.83	0.17	1.50	4.00
Physicians	1.40	1.75	1.40	0.00	4.55	0.00
Nurses	2.33	1.17	0.50	0.00	4.00	0.00
Clerks	1.50	0.50	1.33	1.33	4.67	0.00
Social workers	2.33	0.33	0.33	1.00	4.00	0.00
Technicians	1.50	0.25	0.25	1.50	3.50	0.00
Managers	0.33	0.33	1.17	1.17	3.00	0.00
Total	1.41	0.58	0.85	0.72	3.56	0.62

Mean frequency of occurrence of topics defining IS security

Mean frequency of occurrence of topics presenting the context of IS security

Occupational communities	Healthcare-related context				Tech-related context			
	HIPAA regulations	Stigmatic health conditions	Lack of resources	Total healthcare-related context	Technological change	Increasing dependence on technology	Increasing IS literacy	Total tech-related context
IS professionals	1.17	0.17	0.67	2.00	1.33	1.17	1.33	3.83
Physicians	1.00	0.20	0.20	1.40	0.00	0.20	0.00	0.20
Nurses	0.50	1.33	0.00	1.83	0.00	0.00	2.00	2.00
Clerks	1.33	0.67	0.00	2.00	0.17	0.33	2.00	2.50
Social workers	1.33	1.33	0.33	3.00	0.00	0.00	0.00	0.00
Technicians	0.50	0.00	0.25	0.75	0.25	0.25	0.00	0.50
Managers	1.67	0.17	0.83	2.67	0.17	0.33	0.00	0.50
Total	1.10	0.59	0.33	2.03	0.18	0.33	2.14	2.66

Mean frequency of occurrence of topics defining IS security

Mean frequency of occurrence of topics related to internal threats to IS security from Hospital's organization

Occupational communities	Internal threats: regular organization of work	Internal threats from the use of any medium	Total internal threats from hospital' organization
IS professionals	0.00	0.00	0.00
Physicians	0.40	0.60	1.00
Nurses	0.17	1.50	1.67
Clerks	0.29	0.14	0.43
Social workers	1.00	0.00	1.00
Technicians	0.00	0.25	0.25
Managers	0.00	0.00	0.00
Total	0.26	0.36	0.62

Mean frequency of occurrence of topics related to external threats to IS security

Occupational communities	Tech-related external threats: viruses, spyware	External threats from intruders: hackers	External threats from intruders: intruders in premises	Total external threats
IS professionals	4.83	1.50	0.83	7.17
Physicians	0.00	0.20	0.00	0.20
Nurses	0.50	0.50	0.17	1.17
Clerks	0.00	0.00	0.17	0.17
Social workers	0.00	0.00	0.00	0.00
Technicians	0.25	0.25	0.00	0.50
Managers	0.00	0.17	0.17	0.33
Total	0.85	0.38	0.21	1.44

Employee Comments

- Technician:
  - *"Everybody [is responsible for IS security]. All of us. Everybody who works here has some kind of access to patient information, so anybody could be a potential leak."*
- Physician:
  - *"In the hospital, we have patient care that is confidential. It [patient care] is between a patient and a physician, or with the people who are taking care of this patient. You don't want it to be out in the open."*

Employee Comments

- Manager:
  - *"Sometimes HIPAA is applied a little bit too well. It is practiced and sometimes it gives very funny results…"*
- Nurse:
  - *"Physicians have an access to systems that is different from the one that nurses have. Depending on your title, it determines how much access you get. We know that physicians go get the charts they are not supposed to get and [they] try to change things because they forgot to do something. Sometimes, they steal someone else's password."*

Employee Comments

- IS Professional:
  - *"We have viruses that keep coming in. They can dismantle the hospital's systems within minutes, so we are continuously developing more and more aggressive tools for virus detection, and for intruders. We are doing things of that nature on a daily basis."*
  - *"In my view, you have IS security when you have your computer to work its best."*

Conclusion

- IS Concerns
  - IS Professionals focus on computer attacks.
    - Hackers
    - Malware
    - Security awareness
  - Others on human element.
    - Other employees curiosity
    - Password sharing
    - User responsibility
- Need for better communication on IS concerns

Discussion

- Had there ever been a case of theft of information at the hospital?
- Did other factors effect the answers?
  - the amount of time in the field
  - age
  - personal involvement in an IS incident
- What kind of IS training was provided?
- Only 39 out of over 2,000 employees. That's less the 2%.