HAL
archives-ouvertes.fr

Using Actor Network Theory to Understand Information Security Management

Karin Hedström, Gurpreet Dhillon, Fredrik Karlsson

▶ **To cite this version:**

Karin Hedström, Gurpreet Dhillon, Fredrik Karlsson. Using Actor Network Theory to Understand Information Security Management. Kai Rannenberg; Vijay Varadharajan; Christian Weber. 25th IFIP TC 11 International Information Security Conference (SEC) / Held as Part of World Computer Congress (WCC), Sep 2010, Brisbane, Australia. Springer, IFIP Advances in Information and Communication Technology, AICT-330, pp.43-54, 2010, Security and Privacy - Silver Linings in the Cloud. <10.1007/978-3-642-15257-3_5>. <hal-01054504>

HAL Id: hal-01054504
https://hal.inria.fr/hal-01054504

Submitted on 7 Aug 2014

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution| 4.0 International License

Using Actor Network Theory To Understand Information Security Management

Karin Hedström[1], Gurpreet Dhillon[2], and Fredrik Karlsson[1]

(1) Örebro University, Fakultetsgatan 1, SE-701 82 Örebro, Sweden
{karin.hedstrom,fredrik.karlsson}@oru.se
(2) School of Business, Virginia Commonwealth University,
301 W. Main Street Richmond, VA 23220, USA
gdhillon@vcu.edu

Abstract. This paper presents an Actor Network Theory (ANT) analysis of a computer hack at a large university. Computer hacks are usually addressed through technical means thus ensuring that perpetrators are unable to exploit system vulnerabilities. We however argue that a computer hack is a result of different events in a heterogeneous network embodying human and non-human actors. Hence a secure organizational environment is one that is characterized by 'stability' and 'social order', which is a result of negotiations and alignment of interests among different actants. The argument is conducted through a case study. Our findings reveal not only the usefulness of ANT in developing an understanding of the (in)security environment at the case study organization, but also the ability of ANT to identify differences in interests among actants. At a practical level, our analysis suggests three principles that management needs to pay attention to in order to prevent future security breaches.

Keywords: Information security, Computer hack, Actor network theory, IS security

1 Introduction

There appears to be at least two schools of information security (IS) that largely pursue their own agendas without many cross-references. On the one hand there is the technical school [1, 2] that has to a large extent focused on how technical solutions can prevent IS occurrences, such as computer hacks. However as technologies evolve, a technical fix may not help sustain the solution over a period of time. On the other hand, there is the socio-behavioural IS research [3] that concentrates specifically on understanding managerial and employee attributes that contribute to IS. But, just as technical fixes may not help sustain the solution nor can we rely on administrative procedures alone. Hence, it is prudent to understand IS occurrences, such as hacking, from a socio-technical point of view. Hacking is not only an effect of insufficient technical measures, nor the sole result from bad decisions. In this paper we argue that IS occurrences are

best viewed as socio-technical problems including human as well as non-human actors [4, 5]. By viewing a computer hack as a result of events [6] within a heterogeneous network we will better understand the interplay between the social and the technical, thus increase our possibility to improve the computer security. The purpose of this paper is to illustrate the usefulness of Actor Network Theory (ANT) for understanding computer security management within an organization. In this paper we argue that security breaches and possible negative events are results of a lack of understanding of the complex inter-relationship between different actors. Such actors may be technological or human. While using the case of a computer hack in a public institution, we illustrate the inherent complexities in the interplay between the technical and the social. In a final synthesis the paper proposes that a socio-technical orientation in addressing IS would have helped in understanding the situation and in better managing the sequence of events at Stellar University.

The paper proceeds as follows. Section 2 contains a discussion about the two schools of IS: technical and socio-behavioural. Section 3 describes our use of ANT as research method. Following this, Section 4 provides a short introduction to the hacker case at Stellar University. Section 5.1 reports on our analysis and with this basis we discuss our key findings in Section 6. Finally, the paper ends with a concluding discussion in Section 7.

2 From Technical to Socio-Technical IS Research

IS research can broadly be classified into two categories - technical and socio-behavioural. The technical research has largely been focused on designing sophisticated devices and algorithms to protect the information resources. The socio-behavioural research on the other hand has devoted its interested to the understanding managerial and employee issues related to IS. While both categories of research have merit and over the past several years have made significant contribution to the body of knowledge, there are some fundamental limitations.

Technically oriented IS research has a narrow design focus. The emphasis has been on creating sophisticated artifacts that help in protecting the information resources. Occasionally the technical IS research has made calls for considering the more organizational aspects of IS. For instance Thomas et al. [7] make a call for conceptualizing task based authorizations and Burns et al. [8] in discussing the meaning of security and safety. However, such calls have been rather limited. More often the technical IS community has aspired to develop security mechanisms with little relation to the context of use. This does not mean that technical IS researchers have not undertaken pertinent research. In fact the converse may be true. For instance, the importance of confidentiality as a requirement has always been highlighted and various privacy preserving mechanisms have been developed. In recent years technical IS researchers have had a renewed interest in the confidentiality requirements, particularly because of corresponding advances in computing. Along similar lines, Al-Muhtadi et al. [9] propose an authentication framework in the context of 'active information spaces.', and Myles et al.

[10] proposes a system that allows users to control their location information, thus helping preserve privacy in pervasive computing environments.

While these, among others, may be important discoveries, they are limited in terms of the extent to which the social environment is understood. It is only when a given technology routine gets disturbed that a plethora of problems emerge. Technology routines get disturbed in different ways. At a simplest level, technology can be used to circumvent trust in interactions, causing disturbance in a routine. In August 2009 three individuals were apprehended by the police for gaining access to private details of another individual seeking massage services on Craigslist (www.craiglist.org). Following solicitation, the victim shared all his private details with the accused and ended up getting robbed. A more complex form of technology routine disturbance is when the rule inscribed in a computer based system fails to match those in the organization or the context. Any discordance in these results and security gets compromised. Dhillon et al. [11] illustrate such an occurrence in the case of a malaria research center computer crime situation.

Therefore, while it may be prudent to design technical security mechanisms in response to what the context may demand, it is equally important to understand the natural setting in which various actors act. Problems emerge when the rather stable network of actors get disturbed, usually following some negative event. In an aspiration to grow and have a widespread appeal, Facebook allowed third party vendors to design widgets and applications. Such applications accessed more personal information about users than was necessary. It resulted in Californian and Canadian law suits on the grounds that Facebook was harvesting personal information of users. This lead to Facebook being forced to redefine its authentication and identification policies [12]. The intricate relationships between technology and actors have always been at the center of important discussions. In the context of IS, negotiation between authentication, identification and ownership of data has been identified [13]. This together with an inability to balance the needs and wants of various actors causes potential security breaches [14] and discussion on tensions between technology, security and privacy. Angell [15] has illustrated the notion of negotiation between different actors in terms of technical security access and individual rights.

Some early research in the IS community [16], helped in bringing socio-technical issues to the fore. Further evidence of the importance of human factors was rendered by Segev et al. [17], where aspects of internet security are discussed. While this marked the beginning of an appreciation for considering issues that went beyond the strict confines of technical IS concerns, there has been limited guidance in terms of identifying and articulating socio-technical IS. We believe that ANT [18, 19], is one way forward in dealing with this.

3 Actor Network Theory

ANT has its roots in the field of sociology of science and technology [18, 19], where researchers see knowledge as products of 'network of heterogeneous ma-

terials' [4, 5]. ANT is thus a social theory with the aim to understand the construction and transformation of heterogeneous networks including the social as well as the technical. Using this theory as a frame of reference also makes it suitable as a method for analysis [20]. ANT has successfully been used in the information systems field to examine, for example, the development of information infrastructure [21], the standardization process [22] or for understanding IT development within healthcare [23]. Using ANT makes us view the circumstances around a security breach as a heterogeneous network embodying human as well as non-human actors (or actants) [24]. Furthermore, it also forces us to 'follow the actors' [24] and to identify the associations that link the different actors together forming the network. Stability and social order is the product of a process of negotiation, aligning, or translating, different actants' interests in the network [21] - an actor-network where everything runs smoothly. A working computer systems security solution is, in ANT, a product of negotiation. Different views are translated, and inscribed, into the solution. If or when stability occurs the actants see the network as a whole, forgetting about its parts (i.e., black-boxing). It is not until something happens that forces us to question its workings that we open up the black-box and start investigating the parts.

ANT is a process oriented theory following the constructions of associations within the network. One common approach in ANT research is thus to align a series of events as a timeline [25, 26], using critical events as a way to structure the material and guide the analysis (cf. [6]). A critical event is in our analysis an action that has transformed the actor-network and resulted in, or failed to result in, an inscription that has had import for explaining the events at our case at Stellar University.

ANT includes a number of theoretical concepts that can be used to guide the analysis. We will not use all the concepts in our analysis, but rather a sub-set illustrating how ANT can help us disclose the interest and actions of the different actants in the case of Stellar University. By doing this we will better understand why it was possible to hack the computer systems at Stellar University. Table 1 contains a compilation of the concepts that we use during the analysis. One key feature of ANT is that it does not contain any a priori distinction between human and non-human actors. Both are viewed as active makers of actor networks and are included in the unifying actant concept. Furthermore, networks are changed through translation. A translation is the establishment of a new or changed relation between actants, and can be described as coexisting in a network to achieve a common goal. An example from the IS field is when policy makers agree to include a section on confidentiality in the organization's IS policy, maybe in alignment with the ISO-standard. The translation model refers to the prioritization of interests, which means that things (artfacts, orders, goods) are 'in the hands of people; each of these people may act in many different ways, letting the token drop, or modifying it, or deflecting it, or betraying it, or appropriating it. [...] Each of the people in the chain is [...] doing something essential for the existence and maintenance of the token [...] and since the token is in ev-

eryone's hands in turn, everyone shapes it according to their different projects.' [27]

Often such a translation requires enrollment where an actant seeks to influence how another actant should take its shape, or act, in the network. An example of enrollment in IS is when a security manager tries to influence a user to logout from the computer when leaving the room - because it is important to keep the information confidential. Enrollment and translation can result in inscriptions, where interests are inscribed into written material or technical systems. If we continue our example above, a policy maker and a system administrator can decide to use password protection as a way to implement confidentiality which is stated in the IS policy.

Table 1. Key concepts in the ANT framework used in this study

Concept	Interpretation of the Concept
Actant	An actant is a human or non-human actor that takes the shape they do by their relations to other actants, such as a policy maker, a user and an information system.
Actor Network	A heterogeneous collection of aligned interest, including for example, policy makers, users and computer systems.
Event	An action that has transformed the actor-network and resulted in, or failed to result in, inscriptions that had import for explaining the analyzed situation.
Interest	What an actant wants to achieve with an action, for example what a policy maker wants to achieve with including a section on confidentiality in the IS policy.
Enrollment	When an actant seeks to influence another actant to act in a particular manner. For example, when a policy maker provides arguments to include a specific rule in the IS policy.
Translation	The creation of an alliance concerning a specific issue between human actors and non-human actors, for example, an agreement to include a section on confidentiality in the IS policy.
Inscription	A frozen organizational discourse. For example, the materialization of interests in an IS policy that includes a section on confidentiality.

Considering the purpose of the paper, to illustrate the usefulness of ANT for understanding computer security, we will not cover the complete Stellar University case. We have chosen to analyze the translation process from introducing a specific server until the computer system at Stellar University was hacked. Hence, we focus on the different actants and nine events that formed the computer systems security network at Stellar University. We believe this is the most interesting aspect of this case, since it shows how ANT can be used to analyze current computer systems security solutions and reduce the risk of black-boxing such solutions.

Empirical work for the case was undertaken over a period of 8 months. The purpose of the case study was to understand the intricate relationship between the technology and the human actants. We went into the case considering that the hack occurred largely because of a technical failure, but soon to realize that there were a range of behavioral and process related issues. In a final synthesis, the researchers however began appreciating the intricacies of technology and human actor dependence. All major stakeholders were interviewed, particularly guided by a socio-technical perspective. In all some 32 hrs of relevant interviewing was undertaken.

4 Case Description: Hack Discovered at Stellar University

This case study is based on a series of events, which occurred over a period of two years at the Stellar University. Stellar University is a public educational institution, which contains a diverse range of technologies. In this open and diverse environment, security is maintained at the highest overall level possible. Many of the systems are administered by personnel who have other primary responsibilities, or do not have adequate time, resources or training. For example, if the system is not reported as a server to the network group, no firewall or port restrictions are put into place. This creates an open, vulnerable internal network, as it enables a weakly secured system to act as a portal from the outside environment to the more secured part of the internal network. Some departments work cooperatively, sharing information, workload, standards and other important criteria freely with peers. Other areas are 'towers of power' that prefer no interaction of any kind outside the group. This creates a lack of standards and an emphasis on finger pointing and blame assignment instead of an integrated team approach.

During the time that we followed this case a number of organizational changes took place. A shift in management focus to group roles and responsibilities, as well as a departmental reorganization caused several of the 'towers of power' to be restructured. These intentional changes were combined with the financial difficulties of the province and its resulting decrease in contributions to public educational institutions. The university was forced to deal with severe budgetary constraints and cutbacks.

In this paper we focus on a specific server (which we call server_1). It was running Windows NT 4.0 with Service Pack 5 and Internet Explorer 4. It functioned as the domain Primary Domain Controller (PDC), Windows Internet Naming Service (WINS) server, and primary file and print server for several departments. On a Monday morning in February, the system administrator noticed a new folder on the desktop, and called the operating system administrator at the computer center. Upon signing on locally with a unique domain administrator level user ID and password, there were several suspicious activities that occurred. Multiple DOS windows popped up in succession. The suspicious folder was recreated and the processor usage spiked higher than normal. Antivirus definitions and the antivirus scan engine on the system were current; however the

real-time protection process to examine open files was disabled. The assumption was that this may be the first action a hacker took so that the antivirus product did not interfere with the malware application installation. All of these circumstances added up to one immediate conclusion: that the system had most likely been compromised.

5 Actor Network Analysis of 'The Computer Hack Case'

The understanding of why it was possible to hack the computer systems at Stellar University is illustrated through the negotiation process between key actants. We investigate the translation, or inscription, of their interests through different security measures, into the computer systems. In the analysis we show how actants fail to follow decisions or implement negotiated security measures, as they have other, more prioritized, interests. We also illustrate how the analysis reveals different inscriptions. Section 5.1 contains nine critical events that have in some way disturbed the actor-network or been important for its stabilization. This is in line with the event-based approach to ANT [6], where events are used as a way to structure the analysis, and synthesize key findings. The section below summarizes the analysis from the viewpoint of the events that have resulted in the possibility of hacking into the system. Each event is identified by a unique number. To each event we associate the actant carrying out the action and the the interests that guide them. In addition, we discuss the inscriptions, i.e., the materialization of the involved actants' interests in the computer system, that the events have resulted in. We illustrate the case as a process from the point where the naming of server_1 created problems until the hacker got into the computer system forcing the systems administrator to open up the black box of server_1.

5.1 Negotiating Information Security

As the corporate culture at Stellar University is as heterogeneous as the network itself, together with a lack of standards, there are a lot of opportunities for different actants to create whatever level of security they prefer. The naming of the server_1, which we identified as the first event ('E1') is one example. This name was inscribed into the computer systems as the result of the action of the system administrator. He included an underscore in the system name (i.e., server_1) per his interpretation of the network suggestion. An older version of UNIX bind was utilized for the primary static DNS server by the networking group at Stellar University; hence the underscore was unsupported. There were possible modifications and updates that would allow an underscore to be supported, but these were rejected by the networking group. We identify this reject as the event 'E2'. At the same time we conclude that this technical information was not clearly communicated between the two groups.

The third event (E3) we identified is the networking group's efforts to standardize the server names to include dashes. Nevertheless, the name 'server_1'

became irreversible as the system administrator decided it was too much work to change the naming to 'server-1'. A name change required reinstallations of a database manager and reconfigurations of all the computer systems in the domain. His priority was to 'fire fight' and keep everything running. After this event the University management decided to implement a new organization (E4). They had determined that all servers in the department should be located at the computer center. This aligned with the roles and responsibilities of the computer center to provide an appropriate environment for the servers and employ qualified technical personnel to provide operating system support. Other groups (i.e., application development, database administration, client support) were to concentrate on their appropriate roles, which were much different than server administration. There were attempts to enroll the old systems administrators to support centralization of servers and technical personnel in order to ensure a secure computer system. This was, however, not very successful, as they continued to monitor and administrate the computer systems remotely. Server_1 was anyhow transferred to the computer center with new system administrators.

Minimal system documentation and history were included, and since the new system administrators had not built the systems, reverse engineering was necessary to determine installed software and how the hardware and software were configured (E5). In order to stabilize server_1 the new system administrators scheduled a maintenance window to install Service Pack 6a (E6). However, this attempt was quite disastrous. Windows NT 4.0 Service Pack 6a would not apply and had to be aborted. The system administrators received error message of 'could not find setup.log file in repair directory.' The critical application that used SQL would not launch when signed on locally to the server as an administrator, and had an error. Due to the minimal system documentation the new systems administrator lacked the knowledge to solve the problem. As a result, no inscription was made in the actor network. From a security perspective it meant that the computer system was vulnerable to execution of remote code since the Microsoft Security Bulletin MS04-007 was never installed.

Before next maintenance window research was accomplished to determine how to correct the error messages. Microsoft knowledge base article 175960 had a suggested corrective action for the 'could not find setup.log file' error. Further off-hours attempts finally allowed all service packs and security patches to be applied. This Successful installation is our seventh event (E7). The new systems administrators wanted to make modifications of the servers to bring them up-to-date and more in line with current standards. A joint decision was made between the groups to replace the legacy hardware and restructure the environment in a more stable fashion, which was supposed to result in decreased the vulnerability of server_1 (E8). Several replacement servers were agreed upon, and a 'best practices' approach was determined. At that point, lack of manpower, new priorities, resistance to change and reluctance to modify what currently functioned caused a delay of several months. Hence, no inscription was done at that time.

The final and ninth event is when the 'Ken' is granted access to server_1. This happens before that Monday morning in February. The DameWare trojan

program DNTUS26, had managed to cause unwanted changes in the computer system. Netcat (nc.exe) was an active process, which may have been used to open a backdoor and gain access to the system due to the late inscription of Service Pack 6a and the delayed modifications of the servers (E6 and E7). Additionally, a key was added to the Windows Registry that would reinstall the malware if it was located and removed by a system administrator. Since the primary domain controller was hacked and all of the domain security information was amassed in a hacker-created directory, it was assumed that the entire domain had been compromised. By implementing and running the Trojan program, 'Ken', a hybrid of the trojan software and the human hacker, acted as a delegate for the hacker, and actually managed to disturb the running of server_1.

It is evident from the analysis why it was possible to hack server_1. It was a result of not enough negotiations between different actants, especially the lack of negotiation between the key players within systems administration: old and new systems administrators, the networking group and server_1. There was not enough willingness to discuss and collaborate. The associations between the different groups then became weak, thus making the actor-network vulnerable and instable. Another reason why it was possible to hack server_1 was due to the irreversibility of the computer system. Modifications, for instance changing the server name, were hard to make, and required many resources. This made server_1 an 'immutabile mobile', resistant to change. The hacking, however, forced everyone to open up the black-box of the university computer system and scrutinize its different parts.

6 Discussion of Key Findings

As has been discussed in Section 3, an actor-network is ideally a stable environment. If there is integrity among actions, interests and inscriptions, i.e., there is ongoing negotiation, then the chances of disturbances in the homogeneous network are minimal. The homogeneity of the actor network is in a sense a perfection in the socio-technical design. However this ideal stage is typically hard to maintain. Problems occur and can largely be linked to the manner in which inscription [28] occurred or translation [24] took place. In the computer hack case, we observed issues both in inscription and translation. While Latour [24] does not specifically differentiate between the process of inscription and translation, for one informs the other, conceptually however we can think of the two separately.

6.1 Inscription, Translation, and Socio-Technical Design

Based on our analysis of the computer hack case and the process of inscription and translation, we can identify the following socio-technical issues and the related principles.

The system administrator had the implicit assumption that technology could survive on its own. Attempts to fix the problem were simply ignored. System

administrators are typically constrained by their thinking, relying heavily on quick technical fixes. Principle 1: The implicit theories of human actors tend to rely extensively on the non-human actors, ignoring the importance of the negotiation process between the actants, this resulting in severe security flaws.

The networking group rejected the approach that the system administrator took in ensuring that the 'server_1' naming remained supported. This happened without any effort in understanding the intentions or interests of the system administrator. When the new organization was implemented, there was not enough information to negotiate inscriptions. Principle 2: Preponderance of a non-systemic approach, because of limited conceptualization of actant behavior and interests, leads to misinterpretation of actions and to serious IS problems.

Stellar University as an actant took a rather static view of the computer networks. They considered the various actants - networking group, system administrators, server_1 as static entities. The human actors at Stellar University firmly believed that changing one may not necessarily impact others. This resulted in not considering the socio-technical interactions and the related errors in design. All these were then inscribed into a 'black-box'. Principle 3: A static view of the actants ignores interactions and the related negotiations, which results in highly vulnerable environments.

6.2 Interest, Enrollment, and Socio-Technical Information Security

A key process by which the interest and integrity of actor networks are maintained is enrollment. As Walsham [20] notes, 'successful networks of aligned interests are created through the enrollment of a sufficient body of allies, and the translation of their interests so that they are willing to participate in particular ways of thinking and acting which maintain the network.' This means that alignment of divergent interests is dependent of enrollment of different actors into the network. Failure to do so results in a 'broken' actor-network. Central to the enrollment process is also the associated changes by way of which institutionalization occurs.

In the case of Stellar University the discourses underway between the networking group, the system administrator and the technology (server_1) are examples of enrollment. How successful such an enrollment might be is totally a different matter. Clearly in the case of Stellar University, alignment of interest did not occur. As McLoughlin [29] would have argued, the 'entrepreneurial political activity in enrolling human and non-human actor into the actor-network' was unsuccessful.

As is obvious from the Stellar University case, lack of alignment of interest and adequate enrollment of different stakeholders prevented the formation of a stable actor-network. This had serious consequences, which surfaced when a hacker was able to exploit the server. This means that in order for changes - structural or process - to be successful, all interests need to be aligned, failure to do so results in opening opportunities for abuse. Successful IS related socio-technical change can only be brought about if the new technological form includes stakeholder groups so as to align their interests with technology. Inability to do

so results in potential security compromises. Tensions between different actants need to be resolved for successful organizational change. One way of doing this is to bring technology as well as human actors into the same frame of reference, thus ensuring integrity in the process.

7 Conclusion

Management of information security (IS) is a socio-technical activity. And any change related to IS gets translated as socio-technical change, which needs to be understood both in terms of social and material artifacts. In this paper we have illustrated the use of Actor Network Theory in developing an understanding of the socio-technical changes and the emergent IS problems. Results presented in this paper home in on the core concepts of inscription, translation and enrollment, resulting in three principles that are important for management to have in mind: (P1) the implicit theories of human actors tend to rely extensively on the non-human actors, (P2) preponderance of a non-systemic approach leads to misinterpretation of actions and to serious IS problems, and (P3) a static view of the actants ignores interactions and the related negotiations. These principles illustrate the importance of viewing IS as including the technical as well as the social, within a complex heterogeneous network. While our findings cannot be generalized to all IS situations, they do frame management of IS as a socio-technical problem.

References

1. Denning, P.J.: Passwords. American Scientist. 80, pp. 117–120 (1992)
2. Dymond, P., Jenkin, M.: WWW distribution of private information with watermarking. In: The 32nd Annual Hawaii International Conference on Systems Sciences (HICSS-32). Maui, HI, USA. (1999)
3. Sipponen, M., Wilson, R., Baskerville. R.: Power and Practice in Information Systems Security Research. In: International Conference on Information Systems 2008 (ICIS 2008). (2008)
4. Latour, B.: Technology is society made durable. In: Law, J. (ed.) A sociology of monsters: essays on power, technology and domination. pp. 103–131, Routledge & Kegan Paul, London (1991)
5. Law, J., Bijker, W.: Postscript: Technology, stability, and social theory. In: Bijker, W., Law, J. (eds.) Shaping technology/building society: Studies in sociotechnical change. pp. 290–308, MIT Press, Cambridge, MA (1992)
6. Cho, S., Mathiassen, L., Nilsson, A.: Contextual dynamics during health information systems implementation: an event-based actor-network approach. European Journal of Information Systems. 17, pp. 614–630 (2008)
7. Thomas, R.K., Sandhu, E.S., Ravi, S.S., Hu, Y.: Conceptual foundations for a model of task-based authorizations. 7th IEEE computer security foundations workshop. (1994)
8. Burns, A., McDermid, J., Dobson, J.: On the meaning of safety and security. The Computer Journal. 35(1), pp. 3–15 (1992)

9. Al-Muhtadi, J. Ranganathan, A., Campbell, R., Mickunas, M.D.: A flexible, privacy-preserving authentication framework for ubiquitous computing environments. 22nd International Conference on Distributed Computing Systems Workshops, 2002. Proceedings, IEEE. (2002)
10. Myles, G., Friday, A., Davies, N.: Preserving Privacy in Environments with Location-Based Applications. IEEE Pervasive Computing. 2(1), pp. 56–64 (2003)
11. Dhillon, G., Silva, L., Backhouse, J.: Computer crime at CEFORMA: a case study. International Journal of Information Management. 24(6), pp. 551–561 (2004)
12. Fowler, G.A., Lavalee, A.: Facebook alters privacy controls amid probe. Wall Street Journal. Dow Jones & Company: New York (2009)
13. Backhouse, J., Dhillon, G.: Structures of responsibility and security of information systems. European Journal of Information Systems. 5(1), pp. 2–9 (1996)
14. Halperin, R., Backhouse, J.: A roadmap for research on identity in the information society. Identity in the Information Society. 1(1) (2008)
15. Angell, I.: As I see it: enclosing identity, Identity in the Information Society. 1(1) (2008)
16. Dhillon, G.: Managing information system security. Macmillan, London (1997)
17. Segev, A., Porra, J., Roldan, M.: Internet security and the case of Bank of America. Communications of the ACM. 41(10), pp. 81–87 (1998)
18. Bloor, D.: Knowledge and social imagery. University of Chicago Press, Chicago (1991)
19. Hughes, T.P.: The Seamless Web: Technology, Science, Etcetera, Etcetera. Social Studies of Science. 16, pp. 281–292 (1986)
20. Walsham, G.: Actor-Network Theory and IS research: Current status and future prospects. In: Lee, A.S., Liebenau, J., DeGross, J.I. (eds.) Information systems and qualitative research. pp. 466-480, Chapman and Hall, London (1997)
21. Monteiro, E., Hanseth, O.: Social Shaping of Information Infrastructure: On Being Specific about Technology. In: Orlikowski, W.J., Walsham, G., Jones, M.R., DeGross, J.I. (eds.) Information Technology and Changes in Organisational Work. pp. 325–343, Chapman & Hall, London (1995)
22. Hanseth, O., Jacucci, E., Grisot, M., Aanestad, M.: Reflexive standardization: side effects and complexity in standard making. MIS Quarterly. 30, pp. 563–581 (2006)
23. Bloomfield, B.P., Vurdubakis, T.: Boundary Disputes. Negotiating the Boundary between the Technical and the Social in the Development of IT Systems. Information Technology & People. 7, pp. 9–24 (1994)
24. Latour, B.: Science in action: how to follow scientists and engineers through society. Harvard University Press, Cambridge, MA (1987)
25. Hedström, K.: The Values of IT in Elderly Care Information Technology & People. 20(1), pp. 72–84 (2007)
26. Vidgen, R.,McMaster, T:. Black boxes, non-human stakeholders and the translation of IT through mediation. In: Orlikowski, W.J., Walsham, G., Jones, M., DeGross, J.I. (eds.) Information technology and changes in organizational work. pp. 250–271, Chapman and Hall, London (1996)
27. Latour, B.: The powers of association. In: Law, J. (ed.) Power, Action and Belief. pp. 264–280, Routledge London, UK (1986)
28. Akrich, M., Latour. B.: A summary of a convenient vocabulary for the semiotics of human and nonhuman assemblies. In: Bijker, W.E., Law, J. (eds.) Shaping technology/ building society. pp. 259–264, MIT Press (1992)
29. McLoughlin, I.: Creative technological change: the shaping of technology and organizations Routledge, London (1999)