Title	Access rights as a part of information security in enterprises
Author(s)	Golden, William; Conboy, Kieran; Acton, Thomas; Halonen, Raija
Publication Date	2008
Publication Information	Halonen, R., Acton, T., Conboy, K., Golden, W. (December 13, 2008). "Access rights as a part of information security in enterprises". Paper 254. Paper presented at Association of Information Systems SIGSEC Workshop on Information Security & Privacy (WISP 2008). Paris, France.
Publisher	Association of Information Systems
Item record	http://hdl.handle.net/10379/227

Access rights as a part of information security in enterprises

Raija Halonen
Centre for Innovation & Structural Change
National University of Ireland, Galway
Ireland

Thomas Acton, Kieran Conboy and Willie Golden
Business Information Systems Group
J.E. Cairnes School of Business & Economics
National University of Ireland, Galway
Ireland

Association of Information Systems
SIGSEC Workshop on Information Security & Privacy (WISP 2008). December 13, 2008, Paris, France

Workshop Chairs
Kathleen Greenway
Ryerson University, Canada

Ruth Halperin
London School of Economics, UK

AIS SIGSEC Chair
Gurpreet Dhillon
Virginia Commonwealth University, USA

www.security-conference.org/sigsec

Abstract

This paper highlights the problem with access rights as a part of information security in enterprises with many information systems and their human users. In many organisations, users often write down their user names and passwords, thus enabling outsiders to enter information systems without proper authorisation. Furthermore, access rights commonly remain active after their possessors have left the organisation or after roles in the organisation have changed. In addition, there are instances in enterprises where access rights are managed with severe deficiencies. In this study we discuss a case where this issue was found out to be in a critical state when the organisation planned to extend and specialise its business abroad. Literature exposed several approaches and concepts to be concerned with. In our paper, we introduce how we approached the problem with a pragmatic contextual view. Based on prior research we explored access rights perceived in the enterprise with the help of a pre-study in the mode of a semi-structured questionnaire. The design science based framework described by Hevner et al. (2004) provided us with a solution that satisfied the enterprise in its information security efforts. Instead of describing the artefact, we highlighted the usability of the framework in real life and explained how we applied it in our research project.

Keywords: *access rights, design science, information system security*

Introduction

"Nowadays we use a ladle when giving rights." This statement by an IT specialist in our case organisation represents the state of information security that may be reality in more than one enterprise. This paper discusses access rights as a part of information security in enterprises. One of the most often noted challenge is the difficulty of protecting organisations' data and intellectual property. As there are tools to control who gains access, of prime concerns are technology and security policy in the organisation (Johnston & Goetz, 2007.) So far, enterprises have a number of different solutions to be used when protecting their business information but despite that, they cannot explicitly influence the loss of commercial secrets or confidential information out of their organisation (Saltzer,1974; Swanson & Guttman, 1996; Saint-Germain, 2005; Waxer, 2007). Such problems are hard to resolve: employees must have access to the information in order to carry out their responsibilities in the organisation. The problem is often not access but how information is dealt with. Especially in enterprises, both strong information sharing and strong confidentiality are essential characteristics for access control environments (Oh & Park, 2003).

We express our research focus in the form of the following research question: How are access rights valued as part of information security in an enterprise? We approach the question with the means of design science as introduced by Hevner et al. (2004) who described a framework of environment, IS research and knowledge base (Fig. 1). The paper is structured as follows. First, we introduce the research approach and the framework employed. Then, we discuss the central concepts of the research: all of the concepts are related to access, identity and security and they are needed to build the knowledge base of the research. We then introduce the empirical research expressing several actual citations from the participants. In the discussion we describe the ramifications of the research, and finally provide a conclusion.

Research approach

The main interest was in exploring how access rights are noted and valued as a part of information security in an enterprise. We approached the problem with the help of prior research concerning access rights and identification. We focused on following problem setting: What do access rights mean? How are access rights perceived in enterprises? As an additional output we wanted to produce an artefact that would respond to the inquiry.

To effect the study we employed a qualitative design science that aims to implement a solution to a real world problem. In design science it is significant that the output is both created and studied (March & Smith, 1995). We approached our output from three angles as described in Figure 1 (Hevner et al., 2004). The target organisation (represented as "environment" in the framework) and a literature review helped us to determine a knowledge base. The output was realised as IS research that produces artefacts and theories to be part of existing theory and that is justified and evaluated here..

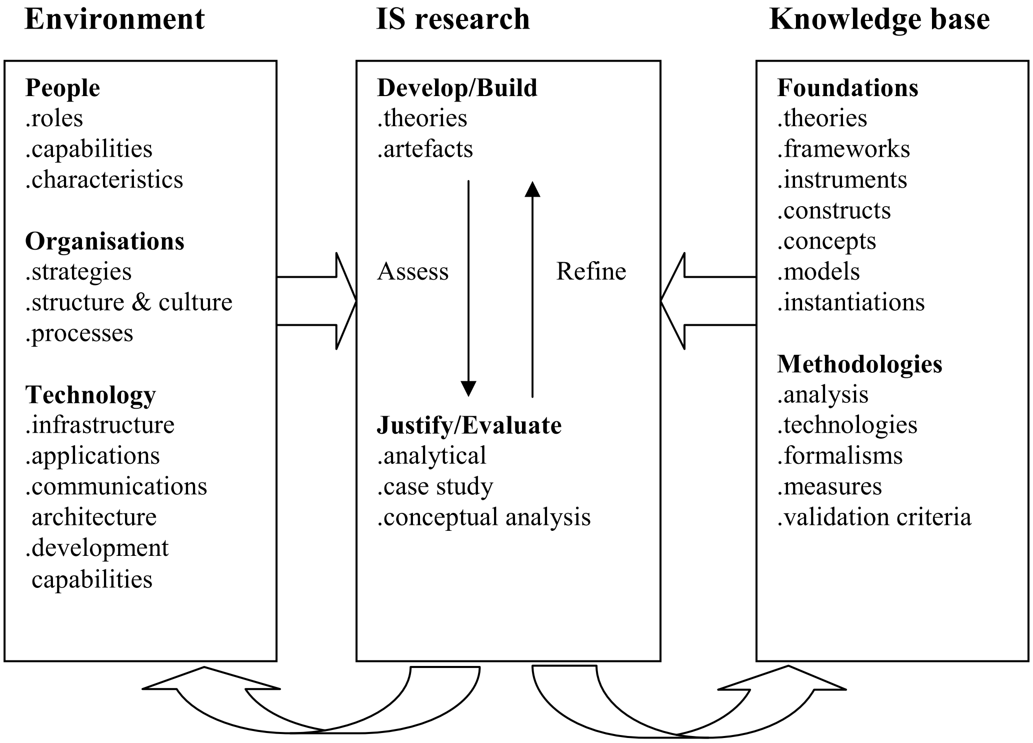

Figure 1. Information systems research framework (adapted from Hevner et al. 2004, 80).

Design science is described as focusing on creating and evaluating innovative information technology artefacts that enable organisations to address important information-related tasks (March & Smith, 1995; Hevner et al. 2004). In this sense, design science approach acted as a problem-solving tool in our research. Hevner et al. (2004) have introduced seven guidelines that arise from the principle that knowledge and understanding of a design problem and its solution are acquired in the building and application of an artefact. These guidelines are:

1. Requirement of creating of an innovative, purposeful artefact
2. Specified problem domain
3. Careful evaluation of the artefact
4. Novel solution
5. Rigorously defined, formally presented, coherent artefact
6. Use of search process
7. Effective communication of research.

Hevner et al. (2004) note that these guidelines are important but are not required to be present simultaneously. The authors want to encourage researchers to be both proactive and reactive with respect to new technology, which is often overemphasised in the artefacts. Furthermore, they encourage the alignment of design-science with real-world production experience. In our research the “artefact” refers to the solution of how access right are managed in an enterprise. In order to find out the desired artefact we needed a pre-study that was preceded by literature review as described next.

The research project was carried out in three interrelating phases: first, a literature review was carried out to investigate the concept of access rights as a part of information security; second, semi-structured questionnaire was addressed to professionals responsible for IT in the enterprise; third, the output was designed and implemented (Fig. 2). We aimed to provide enough evidence given and written out in a manner that any other researcher could interpret the output likewise (Checkland & Holwell, 1998). In our study it was essential that the case study would offer possibilities for learning about and gaining a better understanding of implementations in different environments (Stake, 2000).

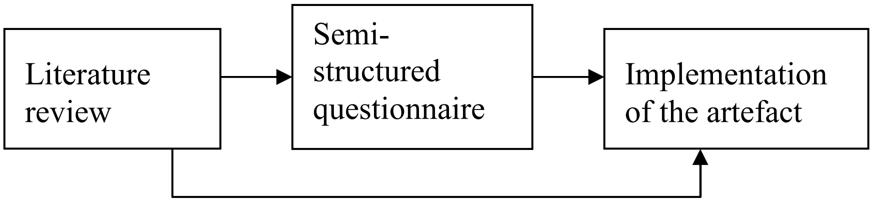

Figure 2. Process of the research with arrows pointing out relations between phases.

Our questionnaire material was collected in February 2008 by using Lotus Similan Survey Manager. The questionnaire was addressed to IT professionals who were in charge of internal information systems in the target enterprise. The total number of addressees was 28 and all of them responded. The goal of the pre-study was to find out the prevailing situation and concept of user rights and information security in the organisation. The questionnaire included 6 closed questions concerning access rights and 10 open-ended questions concerning questions to delineate the future management system. The closed questions were answered with a scale of 1 = no significance (tolerable), 2 = some significance (satisfactory), 3 = medium significance (good), 4 = large significance (very good), 5 = very large significance (excellent).

Prior research

In this section we discuss the context of information system security and access rights grounding on prior research in order to extend the knowledge base (cf. Fig. 1).

Much has been discussed and written over decades about the protection of information assets through the use of information systems. Saltzer (1974) describes how the security issues of his empirical case were laid already in 1960's. Saltzer notes the uniqueness of his case because information protection had influenced the entire system design. He lists principles such as basing protection on permission rather than exclusion and identifies conditions that permit access instead of recognising situations when access should be denied. Furthermore, every access to every object should be checked. The protection should not lie on the ignorance of potential attackers but on protection keys or passwords. Privileges should be granted as well as the interface should be designed so that users routinely and automatically apply the protection mechanisms. Despite passed time, the principles are valid today.

Since 1970's, the discussion has been oriented towards access control. The significance of access control has increased over time due to distributed computing environments where authorised individuals should be allowed to assert their authority over a resource with the scope of their authority (Thompson et al., 1999). Access control is the ability to perform tasks such as reading, writing and execution of system resources and it needs to be managed (Oh & Park, 2003). In their literature review of 46 IS risk articles Sherer and Alter (2004) question if information system risks and risk factors stem mostly from information systems. They point out elements related with risk factors such as inadequate information quality, inadequate information accessibility, inadequate information presentation and inadequate information security. In enterprises, IT superiors agree that improvements in information security necessitate participation from every individual in the organisation (Johnston & Goetz, 2007). Johnston and Goetz further argue that instead of being infused into organisations, information security is engraved in them. Our interest focuses on inadequate information accessibility and inadequate information security and we restrict our study into access rights and their management.

Identification is a key concept in information security. Through identification an object, for instance a user of the information system or an outside process is uniquely individualised. The requirement of identifying objects is justified due to information security. Without identification sharing resources or protecting them cannot be argumented. The object that consumes system's resources, whether a user, an outside process or an application must first be identified and only after that it should be considered which resources should be allocated (Swanson & Guttman, 1996.) So far, the most widespread identification mechanisms are based on passwords, and require that the identifying software has access to the identification information. Therefore, the protective process must be thoroughly documented. Furthermore, the identification information is critical security information that requires strict protection (Allen, 2001.)

In addition to means, identification is a process where one party (also called principal) verifies that the other party is what it claims to be. The other party may be a user, some code to be run or a computer. Identification requires evidence as a mode of credentials. The evidence can be versatile such as a password. After the identity is verified, the party usually wants to use some resource such as a file or a printer. Authorisation refers to functionality that defines if the identified party has right to use resources. Further, some parties have large rights than others (Howard & LeBlanc, 2004.)

There are several concepts used about identifying users. Swanson & Guttman (1996) use “identification” and “authentication”, Lampson (2004) uses “authentication” and “authorisation” while Howard and LeBlanc (2004) use “identifying” and “authorisation”. The terms refer to a method of AAA (Authentication, Authorisation and Accounting). The authentication service aims to recognise the user as a user who has right to use the data net. With the help of the authorisation service the services given to users can be profiled. In other words, the user is authorised to use services provided by the net. With the help of the accounting service it is possible to gather statistics of the user such as time of use (TechTarget, 2007.) However, identification is not the biggest concern. Waxer (2007) comments on the most significant internal threats met in enterprises. An employee may cause damage by sending a ticklish email accidentally to a wrong addressee or on purpose as revenge for perceived injustice or under outside pressure. This possibility is influenced by the level of instructions concerning information security and training or even lack of instructions. In addition, access rights may be too large at that time, the expertise may be too deep or there may be problems with attitude against information security or in motivation. Mallery’s (2006) response to these internal threats is the requirement to sign a non-disclosure agreement even if its only shelter is the legal responsibility in which the employee commits.

As some parties have larger rights as others (Howard & LeBlanc, 2004), access rights should be carefully documented. Saunders et al. (2001) describe a model with access right specified according to roles that can be thought of as job descriptions in an organisational structure. Every user is assigned to a role. This approach enables the procedure of giving permissions that match the organisational policy for the equivalent job.

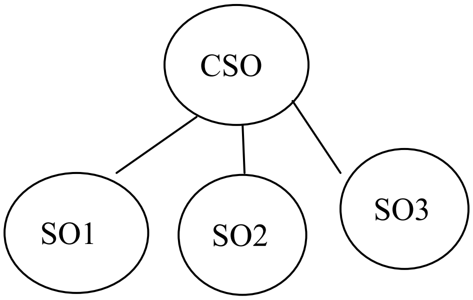

Figure 3. Role hierarchy (Saunders et al., 2001).

In Figure 3 there is a chief security officer (CSO) who inherits roles from three junior security officers (SO1, SO2, SO3). Figure 4 describes an access matrix with different rights related to objects (O1, O2, O3) allocated for the same officers.

	O1	O2	O3
CSO		read, write	
SO1	read		
SO2	read	read, execute	
SO3			read, write

Figure 4. Access matrix (Saunders et al., 2001).

Understanding the significance of admitting rights to users is of extreme importance. Therefore, Barco and Nayyar (2008) recommend that the admittance should be based on user roles and that their management is automatically controlled by the human resources management. The main point is that the management found it to be difficult throughout several enterprises due to the networks of several operation systems. The administrator should be able to manage the methods used in the several system platforms in order to access the appropriate information.

Barco and Nayyar (2008) propose that role-based access control and identity-management are integrated to provide the enterprise capabilities to define and assign roles and to gather information on usage to enable further role refinement (Fig. 5).

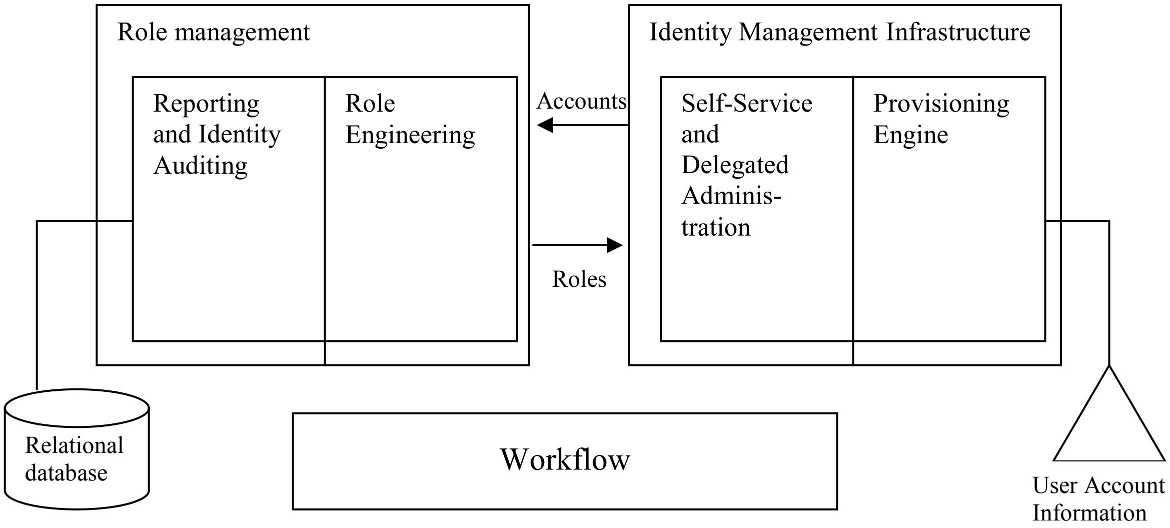

Figure 5. Integrating role management and identity management (Barco & Nayyar, 2008).

There are three grounds for identifying a person: something a person knows, e.g. a password; something what a person has like an ID card; something what a person is such as a. fingerprint (Huntington, 2006). The process of identifying is based on the level of risk. Risky systems require different forms of identifying that very explicitly verify the digital personality. Less risky systems settle for an easier verification (Huntington, 2006.)

When using workstations the users are often identified with the help of identifying service provided by the operating system. In net servers two different methods are used: an identification service in the operating system identifies administrative persons of the server and an identification service of the net software recognises the users of the software. There are identifying mechanisms based both on software and hardware (Allen, 2001.)

When planning an authentication policy it is reasonable to keep in mind that versatile passwords may lead to the undesired situation that users write their passwords on notepads beside their workstations, calendars or wallets. If the notepad with the password written on it comes into wrong hands, there is a potential security risk. If the password policy is difficult to follow the users tend to avoid its use. This kind of procedure easily leads to negative attitude against other security policies, as well (Allen, 2001.) One technique to verify the party and to admit the party to access the resources in an enterprise is to adopt a single-sign-on protocol that aims to reduce the need to remember several user names and passwords (Huntington, 2006).

After the user is identified the user meets access control. Lampson (2004, 39-40) lists five defensive strategies to protect the target: isolate (keep everybody out); exclude (keep the bad guys out); restrict (let the bad guys in but keep them from doing damage); recover (undo the damage); punish (catch the bad guys and prosecute them). Furthermore, Lampson describes a framework to control access with the help of authentication and authorisation that are separated with a guarding reference monitor (Fig. 6).

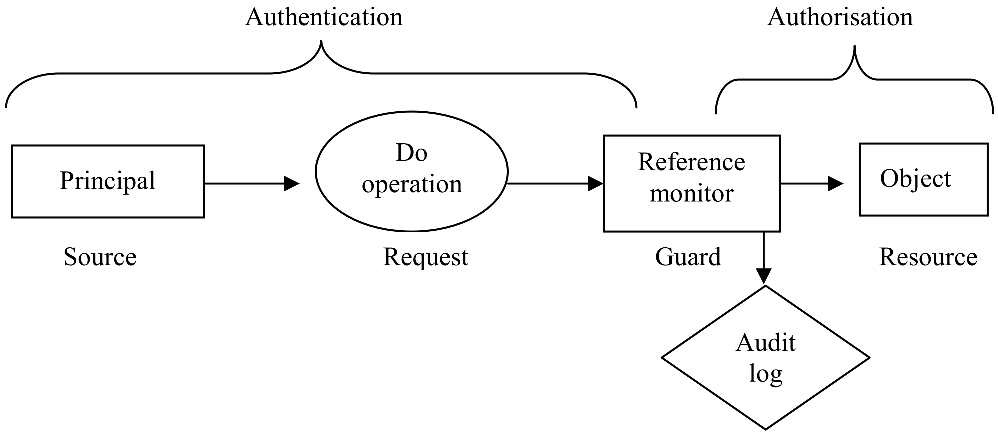

Figure 6. Access control model (Lampson, 2004, 40).

In the access control model by Lampson (2004) the guard uses both authentication information and authorisation information when deciding if the principal is allowed to do its requested operation to the object. The same principle of using a "guard" is described in the research by Halonen (2006) where users from several organisations were identified by a middleware such as Shibboleth. The purpose of Shibboleth is typically to determine if a person using a web browser has a permission to access a resource and thus it aims to prevent problems with unauthorised users (Shibboleth, 2008).

As there are a number of best practice frameworks for organisations to assess their security risks, Saint-Germain (2005) names ISO/IEC 17799 as the most comprehensive approach of all. Saint-German (2005) lists the ten domains of ISO/IEC 17799 in relation to organisational and operational approach. Security policy, organisational security, asset classification and control, compliance, personnel security, and finally, business continuity management can be classified as organisational-driven domains while access control, physical and environmental security, system development and maintenance, and communications and operations management are operational-driven domains.

In all, one can conclude that information security and access control have been widely discussed and in the long run there have been several approaches to manage them.

Empirical illustrations

At that time, the target organisation for this study was one of the world leaders in manufacturing stainless steel. The organisation (called Steelhill) was present in 30 countries and it employed more than 8000 people. Steelhill was to invest in special products of stainless steel in several countries and therefore the need of increased management of access rights and control was in view.

Prior to the beginning of the research project the situation was reflected among the experts in Steelhill through the help of emails. It appeared that there was no proper management of access rights. Therefore, a concern arose about awareness of the role and significance of access rights among both leaders and employees. A meeting was arranged and discussions were held to identify the main goals for the research. The experts were very interested in hearing about management products available.

Prior research (see Fig. 2) gave grounds for the fact that access rights are important and that they must be concerned to protect information property. To be understood, the functionality should be described as a process (Lampson, 2004; Huntington, 2006; Barco & Nayyar, 2008). It was decided that the prevailing process of access rights was to be described in detail in Steelhill, too.

The prevailing situation and need for necessities, requirements and goals of the information system aimed to manage access right were explored by a semi-structured questionnaire (see Fig. 2). Until that time, access rights were applied for with a help of a form in Lotus Domino and it was rather static than responsive. The form followed a simple process which involved the applicant filling out the form and been granted access rights. The most problematic issue was that after applying for access rights the user and system never interacted. Therefore, unnecessary access rights remained in the information systems without a deadline. That problem was realised for instance in cases when users did not use or need the information system anymore. The pre-study exposed:

> *"The biggest problem is that the superiors do not make any requests to remove access rights. I wonder if they know what they should do when a new person comes or another leaves the company?"*

The users also had access in one or several information systems as responded on question about having access in information systems:

> *"The intranet and admitting access rights."*

> *"I have access in so many systems that it is impossible to answer this."*

> *"Lotus Notes."*

Furthermore, the form was not always used but the access rights were applied for by email, telephone, and orally and that caused lacking electronic trace. Requests did not follow the desired approval process. The pre-study exposed:

> *"The superiors cannot use the applying form and they even don't know on which database it is made -> instructions for superiors should be updated!"*

All the questions focused on access rights and related process. Grounding on prior literature, the questions aimed to find out how the users understood or perceived access rights as a concept or their significance (see e.g. Barco & Nayyar, 2008).

The responses to the closed questions are displayed in Table 1. Table 1 indicates that 54 % of the respondents perceived access rights very important and the rest 46 % thought them important. However, one respondent thought the significance of user rights as a part of the information security in Steelhill of no significance. Likewise, one respondent thought that the management of access rights was very weak. Further, one respondent perceived that access rights did not give any protection:

> *"We need a more precise definition of groups and of who belong in them. Nowadays we use a ladle when giving rights."*

Table 1. Responses to close questions with deviations.

Task / Question	St Dev	Mean	Min	Max	N
Evaluate the importance of access rights	0.51	4.55	4	5	22
Evaluate the significance of access rights as a part of the information security in the enterprise	0.99	4.32	1	5	22
On what level is the management of access rights	0.58	2.36	1	3	22
On what level of protection do access right give	1.10	3.41	1	5	22
On what level is the information about access rights	0.95	2.36	1	5	22
Importance of this research	0.94	4.24	2	5	21

Table 1 shows also that only one out of 22 respondents thought that there was enough information about access rights available in Steelhill and all the others perceived that in the enterprise there was a lack of information available about access rights. As a conclusion the table unveils that access rights were perceived important but their management was on a low level.

The responses led to a goal of improving the management of access rights and control with the help of a new information system. Some comments from respondents are:

> *"Definitely explicit rules are needed and an information system that supports the rules."*
>
> *"The removal process of access rights does not work out. It should be linked with HR processes, for example transition announcements or resignation announcements."*
>
> *"What if we had a centralised database where all access rights were available? We could check all access rights by person."*

After the questionnaires were analysed we noted that the management of the access rights needs to be developed and re-assessed, not to mention more precise process defining due to ambiguous and vague routines. According to the received responses, the desired process of access rights would need the department of Human Resources because the process of that time was not properly instructed and the impulse from the superiors was perceived insufficient. The respondents perceived that the process must be started in the human resources, and then be noted by the superiors to be forwarded to the access rights administration and further, to the access rights support to be realised (Fig. 7). The respondents reported:

> *“The applications for access rights are approved too late. The users catch up with calling.”*
> *“The users need to know the password. Likewise they need information if the user rights are allocated or what is the state in there.”*
> *“There are difficulties in HR. IT department has no information if a person is entering or leaving Steelhill.”*

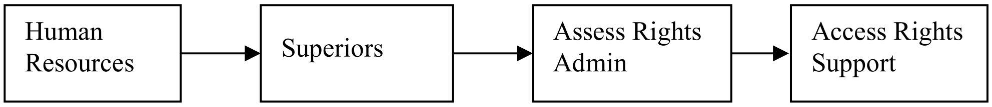

Figure 7. Desired process of access rights.

The implementation (see Fig. 2) included descriptions of the desired access rights process in detail. The descriptions were implemented in one iteration that enabled experts to evaluate the output of the iteration and to give feedback. Only some feedback was given and no changes were needed in the implementation. The feedback was mostly positive. The descriptive verbal and graphical mappings were praised because they illustrated the functionality of the information system clearly and simply enough.

The developed process regarding access rights was tested with the help of five user roles: applicant for access right (“Human Resources”), superior, acceptor of access right (“access rights admin”), user right giver (“access rights support”) and user. After the testing there were some amendments needed and the tests were run again.

The access rights were displayed in an access matrix (cf. Fig. 4) with six levels and six roles where the roles of applying and superior were convergent.

1. The user whose rights were managed could see the access rights form.
2. Human resources had right to request access rights and to see the forms.

3. Superiors had right to modify requests addressed to them, control the state of the requests and to approve them.
4. Application manager had right to approve or dismiss requests to use the application.
5. IT expert with a right to give access rights and to browse requests.
6. System manager with rights to all maintaining operations: maintain access rights, technical modifications to information systems, backups etc.

Discussion

In this paper we aimed to find out about the role and significance of access rights in information security, as seen from an enterprise perspective. To investigate the prevailing conception, a questionnaire was sent to the people responsible for internal information systems. Despite the significance and nature of the enterprise, information security was not properly managed in the organisation. The responses showed that there were severe problems with access rights and their management in Steelhill.

The investigation led us to design and implement an information system to be used when managing access rights in the organisation. The core process of managing access rights necessitated change. Sherer and Alter (2004) argue that instead of IT professionals, the business managers are responsible to insure that information systems support business effectively. Likewise, in our empirical findings the trigger to modify access rights was to come from a centralised department (Human Resources) instead of the superiors of the users in several departments. Figure 8 illustrates the framework that sums up our project. The framework was based on the seminal article by Hevner et al. (2004) that describes a framework for information system research with an environment as the focus of the research, the research itself and the knowledge base that is needed for the research. The framework was formed in the project with finding out the prevailing situation in the enterprise, then designing and implementing a new construction, testing it in the real environment, making amendments according to the testing and building a knowledge base about the related grounds and methodologies.

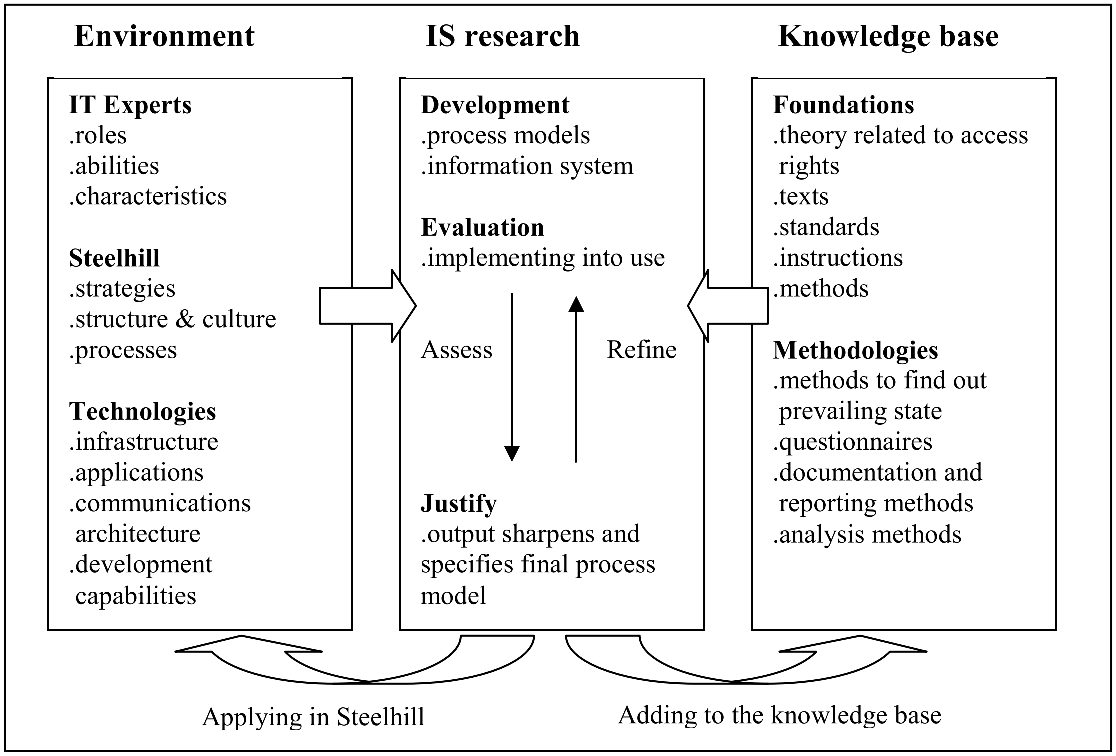

Figure 8. The actual framework.

The link (block arrow) from the Environment to IS research consists of actions that were realised in the pre-study phase and in the discussions when the prevailing situation was found out when current processes were described and deliberated. Likewise, the link (block arrow) from the Knowledge base to IS research refers to actions when usable knowledge was achieved with the help of existing theory, verified processes from literature and by designing a theoretical framework for the research.

In our research, Environment (Fig. 8) consisted of the IT experts of the organisation Steelhill and the technologies that were used in the enterprise. In our case we could recognise a strategic triangle of information security that consisted of people, organisation and technology.

To answer our research question about how access rights are noted and valued as a part of information security our study highlighted the importance of managing properly access rights. The empirical study with responses from the personnel in our target enterprise Steelhill emphasised the need to share information about access rights and related process. The respondents had realised the state of access rights management at that time and they told it in their answers. Talking about ladles when giving access rights to the sensitive information systems in the world-class enterprise only expresses the conception and concern that some of the employees had in the enterprise. Furthermore, the process had to be thoroughly discussed before it could be implemented in the enterprise.

The principles of design science introduced by Hevner et al. (2004) were realised in our research as follows:

1. An innovative and purposeful artefact was needed due to the expanding problem of access rights in the enterprise.
2. A specified problem domain was identified in the enterprise, supported by prior research.
3. The artefact was evaluated carefully by discussing in the enterprise and by testing it. In our case only one iteration was needed due to the descriptive figures adopted from prior research used in the planning phase.
4. The solution was novel in its context as if was not realised until our research had exposed the requirements.
5. The artefact was rigorously defined leaning on prior research on information security and access rights and on the pre-study conducted in our research project.
6. A search process was followed in our research as described in the implemented framework (Fig. 8).
7. Effective communication of research was realised due to becoming acquainted with prior research on access rights and information security.

The concrete output in our research project was an information system that is adaptable in other similar environments, as well. The framework introduced by Hevner et al. (2004) proved to be usable in information system projects such as described in our paper. The output in our research was achieved with a project that included discussions between experts, questionnaires addressed to IT professionals responsible for internal information systems, and with the help of prior research on access rights and information security in enterprises. In all, one can conclude that the chosen approach with design science appeared to support us in achieving a solution that pleased the responsible people in Steelhill.

Conclusion

In our study we focused on access rights as part of information security in enterprises. We aimed to determine how access rights are noted and comprehended by the people working in the enterprise. We approached the research problem with a literature review, used it in our pre-study and ended with information system development (Fig. 2). The framework introduced by Hevner et al. (2004) proved to be suitable in an information system project as described in our paper. Therefore we argue that the framework would contribute comparable efforts in other enterprises, too. We also highlighted the use of simple descriptive figures (e.g. Fig. 3, Fig. 4, Fig. 7) when discussing the prevailing state and the future situation with participants representing the target organisation. Easy figures do enable other parties to get a conception of discussed issues even if the parties are not experienced in the discussed issues. In our case both the prevailing access rights process and the desired access rights process were described in detail with the help of simple figures and this approach made it easy for the participant to get involved in the discussions.

Our research offers interesting issues for further research such as developing the management system to be used in managing access rights in diverse platforms in enterprises. The system developed should be integrated to all information systems in an enterprise and the trigger for actions should come from the users. However, this vision requires more efficient observing, controlling and covering the environment in order to eliminate information security damages. Instead, other larger enterprises should be explored from a similar viewpoint as used in our study. It is worth studying their prevailing state, structure and potential need to develop their access rights systems and their management. Furthermore, more knowledge is needed from the users' view and how they perceive access rights. It might be worth discussing the assumed gap between concepts of information security as perceived by the leaders of an enterprise and by the IT people there.

As we only focused on access rights and found several deficiencies, it would be justifiable to inquiry the state of other components of information security in enterprises with the same approach and framework.

Finally, we want to emphasise the importance of access right as a shelter of enterprise capital. We claim that access rights act as a strong sheltering method when every person in the enterprise has assimilated its significance but on the other hand it can be weak if it is not understood or conformed properly and is not allocated in the enterprise. On the contrary, in such cases access rights may be a threat to the enterprise.

Acknowledgements

The authors are deeply grateful to the people who actively participated in the IS project. Most of all, the input from Marika Vähä-Neijonen deserves our thanks.

References

Allen, J. (2001). CERT Guide to System and Network Security Practices. Canada: Addison-Wesley Longman Publishing.

Barco, J. & Nayyar, S. (2008). Automate Role Management to Avoid Three Major Business Disasters. White paper. Sun Identity Insights. http://www.sun.com/emrkt/campaign_docs/idmgmt/newsletter/0108feature.html. Accessed September 2, 2008.

Checkland, P. & Holwell, S. (1998). Action Research: Its Nature and Validity. Systemic Practice and Action Research 11 (1): 9-21.

Halonen, R. (2006). Building User Authentication in An Inter-Organisational Information System. Journal of Information System Security, Vol 2, Issue 3, 49-68.

Hevner, A.R., March, S.T., Park, J. & Ram, S. (2004). Design science in information system research. MIS Quarterly,Vol 28, Issue 1, 75-105.

Howard, M., & LeBlanc, D. (2004). Writing Secure Code. USA: Microsoft Press.

Huntington, G. (2006). The business of authentication – What is authentication? Authentication World. Huntington Ventures Ltd. http://www.authenticationworld.com/index.php. Accessed September 2, 2008.

Johnston, M.E. & Goetz, E. (2007). Embedding Information Security into the Organization. IEEE Privacy & Security, May/June, 16-24.

Lampson, B.W. (2004). Computer Security in the Real World. IEEE Computer Security, June 2004, 37-46.

Mallery, J. (2007). Hackers Are Not the Biggest Threat to Data: Employees are. Auerbach publications.

March, S.T. & Smith, G.F. (1995). Design and natural science research on information tehcnology. Decision Support Systems, Vol 15, 251-266.

Oh, P. & Park, S. (2003). Task-role-based access control model. Information Systems, Vol 28, 533-562.

Saint-Germain, R. (2005). Information security management best practicle based on ISO/IEC 17799. The Information Management Journal, July/August 2005, 60-66.

Saltzer, J.H. (1974). Protection and the Control of Information Sharing in Multics. Communications of the ACM, Vol 17, Issue 7, 388-402.

Saunders, G., Hitchens, M. & Varadharajan, V. (2001). Role-Based Access Control and the Access Control Matrix. ACM SIGOPS Operating Systems Review, Vol 35, Issue 4, 6-20.

Sherer, S.A. & Alter, S. (2004). Information system risk and risk factors: Are they mostly about information systems? Communications of the Association for Information Systems, Vol 14, 29-64.

Shibboleth. (2008). http://shibboleth.internet2.edu/ Accessed September 4, 2008.

Stake, R.E. (2000). Case studies. In: Denzin NK & Lincoln YS (Eds.) Handbook of Qualitative Research. Thousand Oaks: Sage Publications Inc., p 435-454.

Swanson, M. & Guttman, B. (1996). Generally Accepted Principals and Practices for Securing Information Technology Systems. National Institute of Standards and Technology. Technology Administration. U.S. Department of Commerce, 43-44.

TechTarget. (2007). What is authentication, authorization and accounting? The IT Media ROI experts. http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci514544,00.html Accessed September 1, 2008.

Thompson, M., Johnston, W., Mudumbai, S. & Hoo, G. (1999). Certificate-based Access Control for Widely Distributed Resources. Proceedings of the 8th USENIX Security Symposium, August 23-31, 1999. p. 215-228.

Waxer, C. (2007). The Top 5 Internal Security Threats. IT Security Article 8. http://www.itsecurity.com/features/the-top-5-internal-security-threats-041207/ Accessed September 1, 2008.