# End User Development and Information Security Culture

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

[1] School of Business, Örebro University, Örebro, Sweden
{fredrik.karlsson,karin.hedstrom}@oru.se
[2] Department of Management and Engineering, Linköping University, Linköping, Sweden

**Abstract.** End user development has grown in strength during the last decades. The advantages and disadvantages of this phenomenon have been debated over the years, but not extensively from an information security culture point of view. We therefore investigate information security design decisions made by an end user during an end user development project. The study is interpretative and the analysis is structured using the concept of inscriptions. Our findings show that end user development results in inscriptions that may induce security risks that organizations are unaware of. We conclude that it is a) important to include end user development as a key issue for information security management, b) to include end user developers as an important group for the development of a security-aware culture, and c) to address information security aspects in end user development policies.

**Keywords:** Information security, information security culture, information security policy, end user development, inscription.

## 1 Introduction

End user development grew strong during the 1990s [1, 2]. During this decade end users received powerful desktop tools, such as spreadsheets and easy-to-use databases was used to develop local information systems. This kind of development is highly intertwined with the end users' work. It is, for example, apparent in Brancheau's and Brown's [1] definition of end user development: 'the adoption and use of information technology by personnel outside the information systems department to develop software applications in support of organizational tasks.' Today end user development is a wide spread phenomenon, which exists in almost every organization, although it is not always explicitly recognized, or sanctioned by management or information security specialists. End users are rarely skilled systems developers, and generally lack knowledge about information security practices. End user developed information systems is an important part of many organisations' plethora of information systems, thus making end user development a key issue also when managing information security. In order to develop secure information systems where the organisation's information assets are protected, a security-aware culture, or information security culture, needs to be developed [3]. Information security culture can be viewed as 'the way things are done in the organisations to protect information assets' [4], it is of vital

T. Tryfonas and I. Askoxylakis (Eds.): HAS 2014, LNCS 8533, pp. 246–257, 2014.

importance to include all types of user groups when addressing information security culture. The end user development process and its results are despite this, neither discussed nor addressed as an important issue for an organization's information security culture.

Against this backdrop, the objective of this paper is thus to investigate the role of end user development for an organization's information security culture. We address this objective through the following research questions: (1) does end user(s) make design decisions regarding information security during end user development? and (2) what kind of information security consequences do end users' design decisions result in? Using a case from an international company where an end user developed an information system for price simulation, we illustrate information security consequences that occurred from end user development. This illustration is structured through the use of inscriptions [5] to centre on design decisions (or lack thereof) that have had information security consequences. The conclusions contribute to research on information security culture. Our research acknowledges that end user development has security consequences, illustrating the importance of including end user development as a key issue when working with information security culture. The information security culture becomes an important way of managing information security because end user development is hardly ever controlled as promoted in systems development methods [6]. We also contribute to the end user development field by including information security issues in the on-going debate on pros and cons of end user development.

## 2 Related Research

### 2.1 End User Development

The advantages and disadvantages of end user development have been debated. As end users are rarely skilled systems developers they do not have knowledge about 'best practices' in systems development [2] – not on methods, technical solutions or risks. Also, information security risks resulting from end user development are at best discussed briefly in existing research [e.g. 7, 8]. Most of the criticism to date has focused on the quality of the information systems developed [e.g. 9, 10, 11]. Attention has especially been devoted to spreadsheet models and logical errors in these models, since spreadsheets tools are the most commonly used end user development tool [12]. For example, Edberg and Bowman [13] found in a laboratory experiment that end users were outperformed by information systems students on technical quality. Panko and Sprague Jr. [14] confirmed earlier studies on error rates when building spreadsheet models. While concluding that systems developers have much the same error rate as end users, they do however use extensive time for planned test procedures. While these, among others, may be important discoveries, they are limited in terms of understanding end user development from an information security point of view.

### 2.2 Information Security and Information Security Culture

An important issue for managing information security is the development of an information security culture where employees have the ability to 'integrate acceptable information security practices into their everyday behaviour' [15], i.e., apply a security-aware behaviour to their work [3]. Previous research on information security culture has mainly focused on how to develop or foster 'regular' employees' security-aware behaviour [e.g. 3, 15] or how to improve the systems development processes with regard to information security [e.g. 16, 17, 18]. Information security literature does not explicitly relate to end user development. Instead, this literature either targets end users as consumers of information and information systems or how professional systems developers' work with information security during systems development. In order to make a distinction between use and development we align with Cotterman's and Kumar's [19] definition of development: 'the performance of any or all tasks of the systems development process'. Hence, an end user performing this type of activity differs from end users that consume information and information systems. This means that end user development has to be treated as an activity in its own right. End user developers are thus an important group to address when developing an information security culture, as the end user developed systems could have major information security consequences.

## 3 Research Design

### 3.1 Case Description

The empirical base is an end user development project undertaken in an international industrial company. One major challenge for the company was price analysis and simulations. This had become very time consuming since the company was working on many markets. Information had to be retrieved from several enterprise resource planning systems (ERPs) and quite a large amount of manual work had to be done. For example, each time they calculated new sales prices, they had to remove duplicated information since they were using data from several systems. Considering that they have several thousands product items this was a tedious and error-prone task which took a lot of time. The developed information system was supposed to simplify this task, and integrated different information for price analysis and simulation. One example was the possibility to simulate and compare effects from monetary developments in different countries.

The end user initiated this project based on the problems he had experienced. He was working as area sales manager for several markets and had almost 20 years of experience from the companies' products. As an end user he was very experienced in using spreadsheet software, such as Microsoft Excel. Hence, it was a natural choice for him to build a price analysis and simulation system in Excel. The construction of the system followed the common end user development pattern. It means that the end

user's current understanding of the problem and the design evolved together with his day-to-day work, and was not structured by any systems development method. The end user made major revisions every other month after using it to analyse current prices. However, since the development work was highly integrated in the end user's daily work it is not possible to tell how many person-hours that were spent on this system. The end user developed information system grew from a simple spreadsheet where calculations could be made using multiple currencies, to a solution that integrated several workbooks using Visual Basic for Application (VBA) scripts. The final version of his system used spreadsheets exported from the ERPs. These files were linked manually to the end user's spreadsheet model where automated scripts, for example, removed duplicates based on product number. The end user developed the information system using his laptop, which was not encrypted. All information that was needed for this application was downloaded from the ERPs to this computer and used locally. Price lists, for the markets within the end user's responsibility, were produced from his system and e-mailed to the sales personal in different countries. Hence, this system contained information about the company's margins with regard to specific markets. Since the development work was done as part of his day-to-day work it meant that it was carried out during extensive traveling.

### 3.2 Data Collection

Data sources included one logbook, semi-structured interviews, the information system developed by the end user, and the company's information security policy. Triangulation of data sources provided multiple perspectives [20] on the end user development process, and how to interpret the design decisions. The end user was instructed to write a logbook during his development work. The logbook contained what the end user considered as major design decisions, fulfilment of requirements, and arguments for why these requirements were important. The logbook provided us with a time line of these decisions, but also became an effective means for collecting data and cross-checking the informant's interviews. Four semi-structured interviews were carried out with the end user, during various stages of his development work. We used the end user's log book and the functionality of the end user developed information systems as input for the interviews [20]. Questions addressed the design decisions described in the logbook, and the design rationale behind them. This provided the end user perspective on the development processes. We also obtained access to the end user developed information system. It provided an effective means to validate the informant's logbook during data collection. In particular, it allowed us to identify functionality and security mechanisms that had not been mentioned in the logbook or during the interviews. Finally, we had access to the company's information security policy. It provided information on how to interpret the design decisions made during the end user development process in the light of information security. Furthermore, we concluded that the company did not have a policy concerning end user development.

### 3.3 Data Analysis

The purpose of this paper was to investigate the occurrence of information security consequences resulting from end user development, and to investigate what kind of information security design decisions that an end user make during end user development. It means that we are interested in what types of requirements that are implemented during the development process and why these implementations were made, which makes an interpretative study useful [21, 22]. During the case we unfolded the implementation of requirements through the process of translating [23] design decisions into inscriptions [5, 24]. Inscriptions can be described as a concrete representation of interests and values [25]. The notion of inscription is often used in relation to designers' anticipation of end users' use of a certain technology [24], where the designer delegates patterns of actions, roles, and competencies to future users [26] in for instance an information system. In this study our use of inscription is instead directed towards the end user, and his own vision of future needs and usage. We are interested in a specific type of inscriptions – design decisions concerning information security – taken by the end user. In general terms we define a design decision as an inscription that changes the current version of the end user's information system. As stated above, these decisions are anchored in the end user's interests, what he wanted to achieve through the inscription, which may or may not have been information security related.

The analysis was done in four steps. First we identified design decisions based on the logbook, interviews, and the end user developed information system. For example, the end user added a product name column in the Excel spreadsheet to be able to identify unique products during price analysis and simulations. During the second step we elicited design decisions that had information security consequences. These design decisions could either be implemented as a security mechanism that enhance information security or something that induced security risk/breaches. During this step we used confidentiality, integrity, and availability of information [27], commonly known as the CIA-triad, to classify design decisions as information security related. During the third step we analysed the end user's interest behind each information security-related design decision, i.e. what he intended to achieve from his perspective. Finally, we compared the information security consequence with the company's information security policy in order to analyse if these actions were compliant or non-compliant with the policy. The analysis is presented in Table 1 in Section 4.

## 4 Inscriptions of Information Security

In this section we take a closer look at the inscriptions made by the end users during his nine months of development work, by analysing the final version of the end user developed information system. In total we identified 253 inscriptions made by the

end user. We selected design decisions with information security consequences (see Table 1). The leftmost column in Table 1 contains the number of the design decision, the second column presents the design decision, the third column presents the end users' interest, the fourth column shows the information security consequence, and the rightmost column shows whether or not the design decisions were compliant with the information security policy. When searching for implemented security mechanisms in the end user developed information systems we only identified two. However, we found additional inscriptions that had information security consequences for the organization. These were design decisions that in different ways exposed confidential information for increased risk.

Design decisions 23, 37 and 155 concern downloading information from different ERPs in order to use that information as input in the new system. This information is classified as business critical since it is about current product lines, prices and customers. It was therefore protected in the ERPs using different security mechanisms, such as authorization controls, to keep the information confidential. When accessing these systems from a remote location, i.e. when out traveling, a virtual private network was needed. When the end user downloaded this information as Excel spreadsheet files these security mechanisms became useless. The new information system did not provide any security mechanism to prevent unauthorized access to these files. Moreover, since the laptop was not encrypted these files had no protection at all, beside the login procedure in the Windows operating system.

Table 1 contains six inscriptions (number 28, 65-68 and 74) concerning the margin that the company has on different regions/markets. These design decisions were included in the application to create the simulation functionality and to be able to produce new price lists. Design decisions 189 and 192-193 have a similar purpose in the information system. They were used to create volume discount for different customer segments. Hence, these breakpoints were based on the strategic importance of specific customers. As the developed information systems did not have security mechanisms, and the laptop was unencrypted, it meant that this information was unprotected. The end user used this application in his daily work. The application produced a unique spreadsheet per country (design decision 186). These spreadsheets contained no formulas on how the prices had been calculated; instead they were produced from a second workbook using VBA-scripts. Due to geographic distances the end user e-mailed the relevant price list to the sales personal in each country (design decision 187). Hence, this way of working meant that the end-user implemented a manual security mechanism where a price list for a specific country was treated as confidential information. However, e-mailing the price lists also meant that they were distributed to personnel within the organization that had various, to the end user, unknown security solutions. There is also the risk of entering an incorrect e-mail address, thus disclosing sensitive information to unauthorized people.

**Table 1.** End user's design decisions

| No | Design decision | Interest | Information security consequence | Compliance with information security policy |
|---|---|---|---|---|
| 23 | Download product information from ERPs to integrate in the new system. | To have access to up-to-date data for the analysis | This information is protected by the security mechanisms set up by the security adminis-trator. Extracting this information to the unencrypted laptop decreases the protection. | The end user has the authority to use this information, but not on an unencrypted computer. |
| 28 | Adding margin for region 1. | Necessary for carrying out simulation | Exposing the company's current margin/markup. | The end user has the authority to use this information. |
| 37 | Download product information from ERPs to integrate in the new system. | To have access to up-to-date data for the analysis | This information is pro-tected by the security mechanisms set up by the security administrat-or. Extracting this information to the unencrypted laptop decreases the protection. | The end user has the authority to use this information, but not on an unencrypted computer. |
| 65 | Adding margin for region 2. | Necessary for carrying out simulation | Exposing the company's current margin/markup. | The end user has the authority to use this information. |
| 66 | Adding margin for region 3. | Necessary for carrying out simulation | Exposing the company's current margin/markup. | The end user has the authority to use this information. |
| 67 | Adding margin for region 4. | Necessary for carrying out simulation | Exposing the company's current margin/markup. | The end user has the authority to use this information. |
| 68 | Adding margin for region 5. | Necessary for carrying out simulation | Exposing the company's current margin/markup. | The end user has the authority to use this information. |
| 74 | Adding margin for region 6. | Necessary for carrying out simulation | Exposing the company's current margin/markup. | The end user has the authority to use this information. |
| 155 | Download customer information from ERPs to integrate in the new system. | To have access to up-to-date data for the analysis | This information is protected by the security mechanisms set up by the security administrator. Extracting this information to the unencrypted laptop decreases the protection. | The end user has the authority to use this information. |

**Table 1.** (*continued*)

| | | | | |
|---|---|---|---|---|
| 186 | Producing one unique price list/country | Keeping confidentiality | Price information is kept confidential for sales people belonging to the specific country | The policy does not state that one country's price information should be kept confidential |
| 187 | E-mailing price lists to each country | Keeping confidentiality | Price information is kept confidential for sales people belonging to the specific country | The policy does not state that one country's price information should be kept confidential |
| 190 | Adding breakpoint for first volume discount | Incorporating the company's price strategy in the simulation | Exposing the company's discount model and how it is used. | The end user has the authority to use this information. |
| 193 | Adding breakpoint for second volume discount | Incorporating the company's price strategy in the simulation | Exposing the company's discount model and how it is used. | The end user has the authority to use this information. |
| 194 | Adding breakpoint for third volume discount | Incorporating the company's price strategy in the simulation | Exposing the company's discount model and how it is used. | The end user has the authority to use this information. |

## 5 Discussion

Our analysis shows that the end user made 14 design decisions information security consequences. We only found two design decisions, 186 and 187 in Table 1, that were conscious information security design decisions. The most interesting aspect of design decisions 186 and 187 is that the end user introduced a security mechanism, to keep the price lists separated for each country, which was not necessary according to the information security policy. As we continue examining the design decisions in Table 1 we find inscriptions made into the end user developed information system that decreased information security in existing ERPs. The end user downloaded information about existing products, prices and customers to his laptop, which was stored unencrypted and only protected by a Windows login. Hence, the information was stored in a less secure environment compared to the ERPs. This did not mean that the ERPs as such were compromised. The end user had not disclosed information on how to access them; instead he had moved data outside these systems. From the end user's point of view this was compliant with the information security policy since the Excel exports 'functionality was available in these systems'. According to the information security policy the end user had authorization to use this information, however employees were not allowed to download sensitive information to unencrypted computers. Furthermore, the end user (or any developer) needed clearance from top management in order to combine information from the three ERPs into a new information system. However, this information was only found in the part of the information security policy distributed to systems developers, and hence the end user never made such a request.

From Table 1 we can tell that the end user's design decisions were mainly driven by his needs to solve his current work problems – in this case doing price analysis and simulations when 'creating new or updated price lists'. For example, he added product information from the ERPs to 'have a complete and fresh starting point' in his system. Customer information was downloaded to use the 'different customer categories in the calculations'. The decision to download information as Excel files and linking them manually to his system was preferred 'based on my knowledge of these systems.' However, the end user expressed a concern that this solution was sensitive to 'how these files were created. You end up with nothing but errors if the right data is not found in the right columns'. Hence, this shows that he reflected on the drawbacks of manually extracting data from the ERPs, but not from an information security perspective.

Our findings show that some of the end user's design decisions were non-compliant with the company's information security policy. It means that end user development is not only a quality problem due to end user's limited skills in systems development, which has been the main concern in existing end user development research [e.g. 10, 11, 28, 29], but that end user development also can create information security risks. This illustrates the importance of including end user development as a key issue for a security-aware culture. As we have shown some of the design decisions resulted in increased or new information security risks, exposing information found in the end user developed information system, and information from other, presumed, secure information systems. One problematic aspect of end user development is that it is common in today's organizations, but management rarely controls the development of such applications [6]. Consequently, as end user development results in insecure information systems it means that many organizations, today, have security-compromised systems that they might not even be aware of. When it comes to the information security field it has prioritized end users' use of information and information systems, and how professional systems developers' handle information security during systems development. However, we have identified another area that needs attention: end users' development of information systems. It means that end users are not only consuming information and information systems; they are creating new information and information systems. What complicates matters is that end users have limited knowledge of systems development methods (as in our case), and often do not apply any explicit methods in their endeavors. Consequently, existing contributions in research [e.g. 16, 17, 18, 30] on integrating systems development methods and information security may have limited impact on the situation. It should be acknowledged that an end user (often) develops something only he/she is supposed to use. To some extent this makes the end user's thinking and decisions different from the thinking/decisions made by a professional systems developer. In the former case, when the end user acts as the developer, he/she knows how the 'end user' thinks and reacts to various events since it concerns him/her. This fact may allow the end user to mitigate the need for explicit security measures to some extent, as he/she implicitly rely on the 'end user' to work properly even if no explicit measures are made. On the contrary, professional systems developers lack such luxury and their assumptions on abilities of the 'end user' are naturally limited to some low common denominator, and consequently explicit security measures have to be considered. However, this does not mean that end users, when carrying out end user development, are allowed to violate the

information security policy of the organization. Our findings on end user development should have impact on how organizations work with their information security culture, as well as on how they address end user development. Furthermore, our findings should have an impact of the research agenda in both end user development and information security. When it comes to end user development policies existing research [e.g. 31, 32, 33] does not reveal whether or not these policies address information security. Of course, existing research might not have looked into this area, but it should also be acknowledged that end user development policies seem to be rare in practice in the first place. From an information security point of view end user development is not dealt with as a specific area [e.g. 34, 35-37]. Hence, when end users develop information systems they are governed by the general instructions found in the information security policies and the existing information security culture.

## 6 Conclusion

End user development is a common phenomenon today, where end users develop their own information systems to solve day-to-day problems. Although being extensively researched, the end user development process and its result are neither discussed nor addressed in detail in research on information security culture. In this paper we have therefore investigated the role of end user development for an organisation's information security culture. We address this objective through the following research questions: (1) does end user(s) make design decisions regarding information security during end user development? and (2) what kind of information security consequences do end users' design decisions result in? We traced the inscriptions made by an end user when developing an information system. Only two out of 253 design decisions made by the end user concerned conscious implementation of security mechanisms. However, we did find inscriptions that might cause security breaches. Hence, one could in this case describe them as de-inscriptions from a security point of view. Based on the case findings we propose following tentative propositions:

1. The information security field needs to acknowledge that end users develop information and information systems and explicitly address this as a key issue in information security management, including end user developers as an important group for the development of a security-aware culture.
2. The end user development field needs to acknowledge that end user development has information security as well as information quality consequences, and the former needs to be explicitly addressed in end user development policies.

Every research design has limitations, which should be viewed as opportunities for further research. This study is no exception. Our analysis is based on data from one single case study. Although we triangulated data from one logbook, semi-structured interviews, and code reviews we cannot, and do not claim, that we have identified the complete set of inscriptions of information security requirements. Subsequently, attempts to generalize our results to other end user development projects may not be warranted. However, based on the limited amount of data we have still been able to

show lack of conscious information security related design decisions during end user development. We therefore see interesting avenues for future research on the information security consequences of end-user development. We welcome, for instance, future studies mapping the risks of information security breaches in relation to end user development. We have also found that previous research on information security culture commonly view users as a homogenous group, generally as 'employees'. We believe that a lot would be gained if we in future research could differentiate between different user groups and adjust information security measures accordingly.

## References

1. Brancheau, J.C., Brown, C.V.: The Management of End-User Computing: Status and Directions. ACM Computing Surveys 25, 437–481 (1993)
2. Taylor, M.J., Moynihan, E.P., Wood-Harper, A.T.: End-user computing and information systems methodologies. Information Systems Journal 8, 85–96 (1998)
3. Da Veiga, A., Eloff, J.H.P.: A framework and assessment instrument for information security culture. Computers & Security 29, 196–207 (2010)
4. Veiga, A.D., Martins, N., Eloff, J.H.P.: Information security culture – validation of an assessment instrument. Southern African Business Review 11, 146–166 (2007)
5. 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. Studies in Sociotechnical Change, pp. 259–264. MIT Press, Cambridge (1992)
6. Sutcliffe, A., Mehandjiev, N.: End-User Development. Communication of the ACM 47, 31–32 (2004)
7. McGill, T., Klisc, C.: End-User Perceptions of the Benefits and Risks of End-User Web Development. Journal of Organizational and End User Computing 18, 22–42 (2006)
8. Summer, M., Klepper, R.: Information Systems Strategy and End-User Application Development. ACM SIGMIS Database 18, 19–30 (1987)
9. Ditlea, S.: Spreadsheets can be hazardous to your health. Personal Computing 11, 60–69 (1987)
10. Panko, R.R., Halverson, R.P.: An Experiment In Collaborative Development To Reduce Spreadsheet Errors. Journal of the Association of Information Systems 2, 1–31 (2001)
11. Karlsson, F.: Using Two Heads in Practice. In: Fourth Workshop on End-User Software Engineering (WEUSE IV) ACM Digital Library (2008)
12. Kankuzi, B., Ayalew, Y.: An End-User Oriented Graph-Based Visualization for Spreadsheets. In: Fourth Workshop on End-User Software Engineering (WEUSE IV) ACM Digital Library (2008)
13. Edberg, D.T., Bowman, B.J.: User-developed applications: An empirical study of application quality and developer productivity. Journal of Management Information Systems 13, 167–185 (1996)
14. Panko, R.R., Sprague Jr., R.H.: Hitting the wall: errors in developing and code inspecting a 'simple' spreadsheet model. Decision Support Systems 22, 337–353 (1998)
15. Thomson, K.-L., von Solms, R., Louw, L.: Cultivating an organizational information security culture. Computer Fraud & Security, pp. 7–11 (October 2006)
16. Hitchings, J.: Achieving an Integrated Design: the Way Forward for Information Security. In: The IFIP TC11 11th International Conference on Information Security, pp. 269–283 (1995)

17. James, H.L.: Managing information systems security: a soft approach. In: Proceedings of the 1996 Information Systems Conference of New Zealand (ISCNZ 1996), pp. 10–20. IEEE Society Press (1996)
18. Siponen, M., Baskerville, R.: A new paradigm for adding security into IS development methods. In: Eloff, J., Labuschange, L., Solms, R., Dhillon, G. (eds.) Advances in Information Security Management & Small Systems Security, pp. 99–111. Kluwer Academic Publishers, Boston (2001)
19. Fabian, F., Gürses, S., Heisel, M., Santen, T., Schmidt, H.: A comparison of security requirements engineering methods. Requirements Engineering 15, 7–40 (2010)
20. Patton, M.Q.: Qualitative evaluation and research methods. Sage, Newbury Park (1990)
21. Walsham, G.: Interpretive case studies in IS research: nature and method. European Journal of Information Systems 4, 74–81 (1995)
22. Klein, H.K., Myers, M.D.: A set of principles for conducting and evaluating interpretative field studies in information system. MIS Quarterly 23, 67–94 (1999)
23. Latour, B.: Science in action: how to follow scientists and engineers through society. Harvard University Press, Cambridge (1987)
24. Akrich, M.: The De-Scription of Technical Objects. In: Bijker, W., Law, J. (eds.) Shaping Technology/Building Society. Studies in Sociotechnical Change. The MIT Press, Cambridge (1992)
25. Hanseth, O., Monteiro, E.: Inscribing behaviour in information infrastructure standards. Accounting, Management & Information Technology 7, 183–211 (1997)
26. 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, London (1991)
27. ISO: ISO/IEC 27001:2005, Information Technology - Security Techniques - Information Security Management Systems - Requirements. International Organization for Standardization (ISO) (2005)
28. Davis, G.B.: The Hidden Costs of End-User Computing. Accounting Horizons 2, 103–106 (1988)
29. Teo, T.S.H., Tan, M.: Spreadsheet development and 'what-if' analysis: quantitative versus qualitative errors. Accounting Management and Information Technologies 9, 141–160 (1999)
30. Sindre, G., Opdahl, A.L.: Eliciting security requirements with misuse cases. Requirements Engineering 10, 34–44 (2005)
31. Galletta, D.F., Hufnagel, E.M.: A model of end-user computing policy – context, process, content and compliance. Information & Management 22, 1–18 (1992)
32. Rittenberg, L.E., Senn, A.: End-user computing. The Intenal Auditor 50, 35–40 (1993)
33. Speier, C., Brown, C.V.: Differences in end-user computing support and control across user departments. Information & Management 32, 85–99 (1997)
34. Howard, P.D.: The Security Policy Life Cycle. In: Tipton, H.F., Krause, M. (eds.) Information Security Management Handbook. CRC Press, Boca Raton (2007)
35. Peltier, T.R.: Information security policies and procedures - a practitioner's reference. Auerbach Publications, Boca Raton (2004)
36. Smith, R.: The Definitive Guide to Writing Effective Information Security Policies and Procedures. Createspace (2010)
37. Wood, C.C.: Information security policies made easy. Information Shield, Huston (2001)