Information Security Assessment of SMEs as Coursework – Learning Information Security Management by Doing

Ilona Ilvonen
Novi Research Center
Department of Information Management and Logistics
Tampere University of Technology
Tampere, Finland
ilona.ilvonen@tut.fi

ABSTRACT

Information security management is an area with a lot of theoretical models. The models are designed to guide practitioners in prioritizing management resources in companies. Information security management education should address the gap between the academic ideals and practice. This paper introduces a teaching method that has been in use as coursework for ten years. In addition to the theoretical lectures on information security management issues, the students of the course perform information security assessments of local small and medium enterprises (SME).

The general assessment of the information security status of a company gives the students a view into what the companies have taken into practice and if they have used theoretical models to guide their work. The analysis of the status and suggestions for improvements also teach the students to scale the theory with the size and operations of the company. This is important because usually information security management literature takes the viewpoint of large organizations, whereas the companies that participate in the assessment are small or medium-sized. Course feedback from the students shows that the assignment is perceived to be useful and interesting, and that it works well when paired with the theoretical teaching of the course. The students find working with real companies motivating, and state that they have learned more than they would have learned on a purely theoretical course. The paper discusses experiences from the course to present a teaching and learning method worth experimenting with in other universities.

Keywords: Motivation, Information assurance and security, Experiential learning & education, Student perceptions

1. INTRODUCTION

The information systems field in general, and information systems education in particular, are criticized for the gap between theory and practice (e.g. Klein & Rowe, 2008; Mathiassen and Nielsen, 2008). The gap between the theoretical knowledge gained through research and practice-oriented knowledge is in some areas wide, and it needs to be closed in order to offer relevant education for future information systems professionals.

Information security is an area where the teaching of university students faces many challenges. In some areas teaching defense against technological attacks teaches the students to attack at the same time (Logan and Clarkson, 2005), which causes ethical concerns. In other areas getting open information about information management failures and how they have been overcome is challenging (Dutta and McCrohan, 2002), and thus the teaching may lack real-life case examples. However, the understanding of information security management issues is vital for not only information security professionals, but also all managers in a high-level position (von Solms and von Solms, 2004). In the area of security, the mindset of companies is understandably to reveal nothing outside the company to avoid problems with image or direct information security threats. In this sort of environment, getting good educational material for business and technology students to learn about information security management is a challenge. Case-based teaching is found to be inspiring and it brings about good results among students (Böcker, 1987). When the cases come from real companies, it gives an additional layer of interest and relevance to a student.

This paper describes a university course that answers these challenges by involving local small and medium-sized (SME) knowledge-intensive companies in the teaching. The companies let students come into their premises and perform an interview where one or more representatives of the company are interviewed on information security management issues. The scope of the course is management of information security, and thus the aim of the assignment is

to assess the overall status of information security management in the participating companies.

Information security literature emphasizes the awareness of executives of information security risks and countermeasures (Dutta and McCrohan, 2002; Kumar, Park and Subramaniam, 2008; von Solms and von Solms, 2004). One way to raise awareness of information security is to embed information security issues into the study curriculum of future managers, i.e. today's university students. When a course puts students into a position where they assess the information security status of a company, it forces them to think about the business of that company in addition to the information security threats and countermeasures. Information security management deals with finding the balance between reasonable investments in security and a reasonable level of protection (Bojanc and Jerman-Blažič, 2008; Wang, Chaudhury and Rao, 2008). If students simply study the theoretical ideals of information protection and countermeasures, they may be left with an unrealistic view of information security management.

Information security management skills in the information systems or security curricula are called for by many authors (e.g. Kim and Surendran, 2002; Whitman and Mattord, 2004). The course this paper describes not only answers to this call but also aims for information security awareness of students that will not end up in positions of information security professionals. Awareness about information security threats fosters information security culture in organizations (Lacey, 2010; Van Niekerk and Von Solms, 2010). This assignment teaches students to assess information security from a general perspective. The goal is that the students will understand their own role in maintaining and improving the security status of a company, regardless of what role they have in the company they work for in the future.

In this article, the theoretical perspectives of learning motivation and practice-oriented teaching are briefly discussed. Then the methodology of the empirical study, content analysis, is presented. The main part of the article concentrates on analyzing student feedback on an information security management course. Finally, conclusions based on the analysis are presented.

2. THEORETICAL BACKGROUND

2.1 Learning and its drivers

Learning is a very complex phenomenon that is difficult to approach from one single perspective and claim that this particular perspective explains the learning results of different learners. The complexity of the phenomenon has been addressed by many authors (e.g. Simons, Dewitte and Lens, 2004; Haggis, 2004), and it has been approached from many perspectives. For example, the element of student engagement as a driver for learning has been examined as something that should be actively considered in higher education (Zepke and Leach 2010). Although the complexity of the phenomenon of learning is acknowledged, a simpler approach to learning needs to be taken so that learning can be examined at all. If no simplification was done at all, it would mean that learning could not be studied, since the complexity would render the study impossible to carry out. In this paper, the simplification is performed by approaching learning results from the perspective of motivation and practice-orientation.

In universities, the attention of teachers is often on teaching rather than learning (Cegielski, Hazen and Rainer, 2011; Saulnier et al., 2008). The teacher-centered paradigm of teaching refers to the prevailing setting where the instructor provides information and the students passively listen (Barr and Tagg, 1995). Over the years, there has been a shift from the teacher-centered paradigm toward a learner-centered paradigm (Watson and Reigeluth, 2008). The role of the teacher has shifted from an information provider toward that of a coach or learning facilitator (Barr and Tagg, 1995; Saulnier et al., 2008; Watson and Reigeluth, 2008). Although this paper does not address learning entirely from the learner-centered paradigm, framing an assignment from the point of view of the students, and their motivation, is considered a relative approach to the learner-centered paradigm.

Motivation is one element that is considered a driver for good learning results (Kember, Ho and Hong, 2008). Motivated students believe they can achieve the set learning goals and are engaged in the courses that they take (Zepke and Leach, 2010). Motivation is considered vital to learning, but it is something that cannot be addressed directly. Instead, motivation is the result of activities or processes that involve both the teacher and the students (Haggis, 2004; Zepke and Leach, 2010). This is why it needs to be taken into account that not all students are motivated by the same kind of actions. Students with different learning styles (Kolb and Kolb, 2005) may be motivated by different aspects of teaching. However, studies have shown that practical relevance is one common element that increases motivation to learn (Kember, Ho and Hong, 2008).

2.2 Practice-oriented teaching

Case-based teaching motivates students and leads to better learning results than plain lectures (Böcker, 1987). There are variations on what is considered case-based teaching. One way to teach with cases is to use a written case description that students read and then work on to solve a problem described in the case (Böcker, 1987). Another approach is to simulate real-life cases that consultants work with in practice (Merhout, Newport and Damo, 2012). The simulation brings the case to a more practical level and gives students a better understanding of what kind of methods they will work with after they have graduated. Simulations engage students well and they also motivate them to learn the theoretical elements of the courses (Merhout, Newport and Damo, 2012). However, setting up a simulation takes a lot of effort, and still many students may feel that the problem they need to solve is not real, and their work is thus not relevant. For example, Merhout, Newport and Damo (2012) describe the trust in the relevance of a simulation as a major element of a simulation exercise.

The approach of the assignment described in this paper is to give the students an opportunity to identify and solve real problems in existing companies. The risk in this approach is that the students do not identify all the shortcomings, and thus leave matters unattended in their reports. The benefit of working independently with real "customers" and providing

them with solutions that are based on theories learned in class is, however, seen to outweigh this risk. This can be seen as one way of ensuring the relevance of the assignment (Merhout, Newport and Damo, 2012) and empower the students to believe that they are capable of producing a good report (motivation and agency described by Zepke and Leach, 2010).

3. METHODOLOGY

This paper describes a qualitative study that examines feedback material and experiences from a university course through the theoretical lens described in the previous section. Qualitative content analysis of course feedback is carried out in order to identify what kind of issues students bring up as supporting or hindering factors to their learning in the course of information security management.

According to Weber (1990), content analysis can be used for many different purposes with qualitative material. One of these purposes is to use it for revealing the focus of individual, group, institutional or societal attention (Weber, 1990). In this study, the purpose is to find out how the students have found the course assignment, and what kind of issues they mention as feedback of the assignment and their learning from it.

The aim of content analysis is to classify the vast amount of words in qualitative data into a lot fewer content categories that carry similar meanings (Weber, 1990). This means that the analysis method is used to condense the rich qualitative data into a small enough amount of textual categories, so that it maintains the richness of its qualitative nature, yet is easier to grasp and understand. As Weber (1990) states in his book, "there is no right way to do content analysis". This means that the actual practical steps of how to perform the analysis need to be chosen by the researcher based on the material that is analyzed and the research questions that need to be answered (Weber, 1990; Robson 1993, in Elo and Kyngäs, 2008).

In this study, the student feedback is analyzed with the help of a qualitative analysis tool, Atlas TI. This tool was used to categorize the student feedback into content categories that carry similar meanings. Inductive, or conventional, content analysis emphasizes that the categorizations are formed as the analysis progresses. This means the categories emerge from common coding of the material by grouping similar codes together (Hsieh and Shannon 2005).

Writing feedback is part of the course for participating students. The students give feedback in free form and openly with their own name. This sort of feedback has been a part of the course for academic years 2010-11, 2011-12 and 2012-13, and this paper analyzes the feedback from these three years. A total of 63 students gave their feedback during this time.

Usually teachers gather feedback on teaching via anonymous questionnaires. The problem with these questionnaires is that only a few students choose to answer them, and comprehensive feedback, negative or positive, is difficult to achieve. Openly given feedback may filter away negative opinions, because the students cannot hide behind anonymity. However, the encouragement of constructive criticism has resulted in feedback that also voices negative feelings about the course teaching. The negative opinions were mostly related to issues other than the assignment, which is the focus of attention in this paper. At the beginning of each course, the teacher presents what kind of changes have been made to the course arrangement as a result of student feedback. This encourages the students to write constructive feedback, because they can see that it has had a practical impact.

The following questions guide the students when they give their feedback (the questions are translated from the native language of the students):

- Course teaching in relation to your learning style: Did the teaching support your learning? Did you attend lectures, why? How would you improve teaching on the course?
- Assignment. What was good about it, what needs improvement?
- Exam. Did the exam measure your learning? Was preparing for the exam useful for you? How could the exam be improved?

These questions help structure the feedback, but they also help the students analyze their learning on the course. The point of view of improvement encourages the students to analyze whether they would have learned better in some other way. Instead of a negative expression of what was not good about the course, the students are asked to state what could be improved. This challenges them to provide a reason why they have a negative opinion of a teaching element.

4. EXPERIENCES FROM A COURSE

4.1 Assignment

The information security management course brings students with diverse backgrounds together. The course is a part of the study curriculum for both information technology students with a minor in computer security, and for information and knowledge management students with a major in information management, knowledge management or logistics. Some students from other study programs opt for the computer security minor, and participate in the course in addition to the two main groups. The diverse backgrounds of the students challenge the teacher to approach course topics from angles that are new and interesting for all, yet comprehensible without extensive primary knowledge on the subject. The course assignment that applies information security management principles to an existing company serves this purpose well.

Each year, a different group of local information- or knowledge-intensive SMEs are contacted and asked to participate in the information security assessments. The companies receive an offer for an opportunity to give an interview to students. In return for their time, the company receives a report from the students that addresses their main shortcomings of information security management, and how the company could improve their information security level. In many companies, the interview itself has served the purpose of triggering discussions on areas that may need improvement. These companies may have put the

improvements into practice even before the students have finished writing their assessment reports. Each year there has been enough willing companies to participate in the interviews, so that each group of 3-4 students has a company to assess.

Information security assessment frameworks form the basis for the assessment interviews (ISO, 2005; Kairab, 2005; Kumar et al., 2008). The students receive a question set that they need to use in the interview. The teacher formulates the questions and updates them slightly every year on the basis of experiences from the previous years. Changes in the environment and technologies have also caused changes in the question set. For example, the use of social media has emerged as a potential source of information threat to a company, and thus social media has been added as a theme in the assessment questions. The focus is on the general management of information security, and thus the assessment does not include a technical audit of information systems. The interview questions are included in Appendix A.

The teacher prepares the students for the interviews by going over the interview questions in class beforehand. The students are also expected to analyze the questions and alter them slightly in case the questions are not entirely suitable for the company that they interview. The teacher encourages the students to come up with additional questions if they feel like it and if there is time for them. This preparation is designed so that the students have thought ahead about how they are going to report the interview and why they ask the questions they use. The preparation by course staff resembles mentoring used on other courses (Merhout et al., 2012) but in the case of this course, the student groups work quite independently in the interview and with the report.

The students receive a report template to structure their report and analysis in addition to the interview questions. They also have the possibility to ask for advice from course staff while writing the report. Only a few groups have chosen to opt for the advice; most groups have embraced the opportunity to work on their own in preparing the report. The results have been generally good, and only a few reports have had to be improved before handing them to the company. The assessment assignment has been carried out ten times, and a total of 129 groups have completed their final report. Some of the companies that have participated in the interviews have done so several times, so the total number of companies over the years is smaller.

The companies also receive a summary report on the assessment. The summary report compares the interview results across companies. In this summary report, the companies appear anonymous, so that no company-specific information is revealed to anyone other than the student group responsible for the assessment on the company. The course staff prepares the summary report after assessing all the group assignment reports. This summary report has worked well as an introduction to qualitative data analysis for the research assistants working on the course each year. The participating companies can benchmark their information security status on the basis of the summary report. The summary report is also the reason for giving students the set question and a report template. Before the creation of the template, the summary report was challenging to prepare, since every student group chose the topics they felt were necessary to write about in their report. This led to missing data from the point of view of the summary report. The report template guides students in their work and ensures that the student reports are homogeneous enough to summarize.

4.2 Positive elements of the assignment

All the students that gave feedback in the last three years considered the assignment a positive experience. Most commonly they described the assignment as interesting. Although the term interesting may not always refer to a positive expression, in the context of the student feedback the positive meaning was clear. Other positive expressions the students used to refer to the assignment were that it summarizes the course well or it is a good way to learn about information security management. Some students chose to describe the assignment simply using the term good.

In addition to the general positive feedback all the students gave, some of the students specified elements that they felt made the assignment a positive experience. These elements are listed in Table 1.

Element mentioned by students	Instances (n=63)
The assignment was a good way to apply theory to practice	31
The context of the assignment generated extra motivation to perform well in the assignment	17
The assignment was beneficial to the company	8

Table 1 Positive elements of the assignment

The most common positive element the students addressed was that the assignment was a good way to apply theory to practice. 31 students mentioned this in their feedback. They feel that the assignment complemented the theoretical content of the course well with the opportunity to apply the theory to the practical context of a real company. The lectures received mainly positive feedback, but the positive element of the lectures was not the theoretical teaching; rather it was the discussions and examples given in class, i.e. the learner-centered content. The assignment extended this practical line to the context of individual companies.

> "The assignment was a good experience. It helped to understand things in practical terms, and showed how real companies have thought about information security. Because the assignment was done for the company, I wanted to put in extra effort and do it as well as I could."

The previous quote from the feedback shows an example of the above-mentioned elements: at first the student states that the assignment was a positive experience. Then he describes the element of putting theory into practice. In the last sentence of the quote, the student further describes how the assignment context motivated him to study harder than

he would have done if the assignment were just a theoretical one.

> "The assignment was one of the most interesting that I have done during my studies. Getting to know the information security solutions of a real company was inspiring and taught me a lot. It was really motivating to do the assignment for a real company."

Seventeen out of 63 students stated that doing the assignment for an existing company added extra motivation for them to perform well in the assignment. They felt that they wanted to prepare a good report for the assignment, so that it would be useful for the company that receives it.

Eight students described that they felt the assignment was useful to the company, and this improved the relevance of the assignment. Although the categorizations presented in Table 1 can be seen to overlap somewhat, the distinction is still made, since some students only stated that they felt the real context of the assignment added motivation, whereas some other students mentioned that it was clearly beneficial for the company, but they do not explicitly mention that this improved their motivation.

Overall, based on the student feedback, it is safe to assume that an assignment with a practical orientation improves motivation. The students feel that the assignment complements theoretical teaching and gives them an opportunity to apply theory into practice, which helps them to understand often difficult theories. Students have given mainly positive feedback about the assignment, and report that the assignment has motivated them to learn. It has also enabled them to apply theory to practice, which helps to understand the often difficult theories. Other studies presented in section 2 also support the proposition that the practical relevance of teaching and assignments increase student motivation (Kember, Ho and Hong, 2008; Zepke and Leach, 2010).

Whether the students have learned more than they would have with a theoretical assignment is unclear, but the feedback shows tentative evidence that the students feel they have learned more. This study, however, does not provide a means to fully analyze the aspect of learning results. Studies have shown that an interest in a topic facilitates motivation, and motivation affects learning results (Schiefele, 1991). Thus it is possible to propose that the assignment turns out good learning results, because the students find the assignment interesting and motivating.

4.3 Main points for improvement

Although the feedback the assignment received was mostly positive, some students provided constructive criticism on how it could be further improved in their opinion. The main points for improvement are listed in Table 2.

The main area of improvement for the assignment is the assignment instructions. Although the instructions are updated and improved from year to year, there is room for improvement in them according to many students. Eleven students mention the instructions overall as being unclear and five students specify that the course teacher should offer more guidance on how to conduct the interview and how to report the findings.

Element mentioned by students	Instances (n=63)
The instructions for the assignment should be improved	11
The teacher should give more face-to-face instructions	5

Table 2 Elements that need improvement

> "You could improve the assignment by offering more instructions at the beginning. In my case a lot of questions were left unasked, because I did not realize until writing the report that they would have been worth asking at the interview."

In the above quote, a student has realized after conducting the interview that the group should have asked more questions. The students are prepared for the assignment in the lectures, but the problem is that the lectures are not compulsory, so not every student receives the instruction. The timing of the assignment instructions could be changed so that it would be nearer to the interviews. In the previous implementations, the instructions for the assignment have been given toward the beginning of the course. The assignment interviews, however, take place after the lectures and after the students have taken their final exam. When the students receive the assignment instructions the assignment may feel too far away, and some students may neglect them. The instructions could also be more interesting for the students if they describe experiences like the previous quote. In that format, they would motivate the students to prepare better in advance.

The students on the course are both bachelor's and master's level students, and the reason for the poor comprehension of instructions for some of the students may be their inexperience in writing assignment reports overall. If a written assignment is not familiar to them in general, then conducting an interview and reporting on the findings may be a big challenge. For other students that are more accustomed to solving and reporting case assignments, this is not a problem.

In summary, the critique that the assignment has received from the students is directed at the instructions the course staff give to the students. Some students feel that their independence in working with the company in the assignment is a positive thing. Some other students feel that they should receive better instructions on how to carry out the interview and how to analyze the interview results. The format and timing of the instructions should thus be more appropriate to the students. In the case of this course, the assignment instructions could be given right before the interviews rather than at the beginning of the course. The better timing of instructions might improve the reception of the instructions, even if their format stays the same.

5. CONCLUSIONS

This paper has described an assignment that puts information security management theoretical teaching into practice with an information security assessment. In the assignment, student groups get an opportunity to analyze the operations of a company, and apply the theory they have learned during the course to the context of that company. On the basis of their interviews with the company representatives, the students make an assessment of the information security status of the company and provide suggestions for improvement. Students have found this assignment to be useful and interesting, and a good way to bridge the gap between theory and practice.

The paper presents an assignment type that could be useful for teaching not only information security management but other topics too. In information security management, the contribution of the assignment is twofold: for some of the students it gives an insight into how they could approach organizing information security assessments as future information security professionals. For other students it works as a way to increase awareness of information security issues, and the kind of problems companies can have with it. Students that have participated in carrying out an assignment like this may be more likely to react positively to information security training and assessments in the future, regardless of their role and position in a company. This conclusion cannot be verified based on this paper, but future studies could address the effect of different kind of security assignments on the students' subsequent awareness of and attitudes toward information security.

Future studies could also address the contributions of the assignment from the company perspective. Up to now, course staff have not received feedback from the companies. Willingness to participate in the assessment is one way to communicate that the companies like the assessment, and thus consider it positive. A more systematic way to collect feedback from the companies could help further improve the assignment. Follow-up interviews by course staff after the company has received their assessment report could be one way of getting feedback from the companies.

This assignment gives an example of co-operation between the business world and academia. Academic teaching should concentrate on established theory, but the connection to the real world where the theories are applied should remain close. Taking a step from case studies to more concrete real-world problems is one way of motivating students. This sort of motivation could be utilized in teaching more. The topics for which this sort of assignment could be useful are not limited to information security management. For example, the information management processes and information flows or information systems architecture could be areas where a similar kind of assignment could be both useful for a participating company, and interesting and motivating for a student group.

ACKNOWLEDGEMENTS

The author wishes to thank Prof. Samuli Pekkola from Tampere University of Technology for valuable advice in writing this paper. The comments of the anonymous reviewers at JISE were also invaluable in improving and finalizing the manuscript.

REFERENCES

Barr, R. B., and Tagg, J. (1995). From teaching to learning: A new paradigm of undergraduate education. Change, 27(November/December), 12-15.

Böcker, F. (1987). Is case teaching more effective than lecture teaching in business administration? an exploratory analysis. Interfaces, 17(5), 64-71.

Bojanc, R., and Jerman-Blažič, B. (2008). An economic modelling approach to information security risk management.International Journal of Information Management, 28(5), 413-422.

Cegielski, C. G., Hazen, B. T., & Rainer, R. K. (2011). Teach them how they learn: Learning styles and information systems education. Journal of Information Systems Education, 22(2), 135-146.

Dutta, A., and McCrohan, K. (2002). Management's role in information security in a cyber economy. California Management Review, 45(1), 67-87.

Elo, S. & Kyngäs, H. (2008). "The qualitative content analysis process".Journal of Advanced Nursing.vol. 62, no. 1. pp. 107-115.

Haggis, T. (2004). Meaning, identity and 'motivation': expanding what matters in understanding learning in higher education?. Studies in Higher Education, 29(3), 335-352.

Hsieh, H. & Shannon, S. (2005). "Three Approaches to Qualitative Content Analysis". Qualitative Health Research.5 (November), 1277-1288.

ISO 27001, Standard on Information Security Management Requirements U.S.C. (2005).

Kairab, S. (2005). A practical guide to security assessments. Boca Raton: Auerbach.

Kember, D., Ho, A., and Hong, C. (2008). The importance of establishing relevance in motivating student learning. Active learning in higher education, 9(3), 249-263.

Kim, K., and Surendran, K. (2002). Information security management curriculum design: A joint industry and academic effort. Journal of Information Systems Education, 13(3), 227-236.

Klein, H. K., and Rowe, F. (2008). Marshaling the professional experience of doctoral students: a contribution to the practical relevance debate.MIS Quarterly, 32(4), 675-686.

Kolb, A. Y., and Kolb, D. A. (2005). Learning Styles and Learning Spaces: Enhancing Experiential Learning in Higher Education. Academy of management learning & education, 4(2), 193-212.

Kumar, R. L., Park, S., andSubramaniam, C. (2008). Understanding the value of countermeasure portfolios in information systems security. Journal of Management Information Systems, 25(2), 241-279.

Lacey, D. (2010). Understanding and transforming organizational security culture. Information Management & Computer Security, 18(1), 4-13.

Logan, P. Y., and Clarkson, A. (2005). Teaching students to hack: Curriculum issues in information security. ACM SIGCSE Bulletin, 37(1) 157-161.

Mathiassen, L., and Nielsen, P. A. (2008). Engaged scholarship in IS research. Scandinavian Journal of Information Systems, 20(2), 3-20.

Merhout, J. W., Newport, S. L., andDamo, P. E. (2012). Simulated audits to engage students in IT governance and assurance courses.Journal of Information Systems Education, 23(2), 113-118.

Saulnier, B. M., Landry, J. P., Longenecker, J., Herbert E., and Wagner, T. A. (2008). From teaching to learning: Learner-centered teaching and assessment in information systems education. Journal of Information Systems Education, 19(2), 169-174.

Schiefele, U. (1991). Interest, learning, and motivation. Educational Psychologist, 26(3-4), 299-323.

Simons, J., Dewitte, S., and Lens, W. (2004). The role of different types of instrumentality in motivation, study strategies, and performance: Know why you learn, so you'll know what you learn!.British Journal of Educational Psychology, 74(3), 343-360.

Van Niekerk, J. F. and Von Solms, R. (2010).Information security culture: A management perspective. Computers & Security, 29(4), 476-486.

von Solms, B., and von Solms, R. (2004). The 10 deadly sins of information security management. Computers & Security, 23(5), 371-376.

Wang, J., Chaudhury, A., and Rao, H. R. (2008). A value-at-risk approach to information security investment. Information Systems Research, 19(1), 106-120.

Watson, S. L., and Reigeluth, C. M. (2008). The learner-centered paradigm of education. Educational Technology, 48(5), 42-48.

Weber, R. (1990). Basic Content Analysis.2nd ed. Sage, London.

Whitman, M. E., and Mattord, H. J. (2004). Designing and teaching information security curriculum. Proceedings of the 1st Annual Conference on Information Security Curriculum Development.

Zepke, N., & Leach, L. (2010). Improving student engagement: Ten proposals for action. Active Learning in HigherEducation, 11(3), 167-177.

AUTHOR BIOGRAPHIES

Ilona Ilvonen M.Sc.(eng) is a teaching associate at Tampere University of Technology. She has seven years of experience in teaching the course that is described in this paper. In addition to information security management, her teaching experience includes also information and knowledge management. She has published her research on information security management and knowledge management areas in several conferences. She is finalizing her doctoral studies at TUT and is due to receive her doctoral degree in information security management and knowledge management during the academic year 2013-2014.

Appendix A.

Interview questions the students receive
Translated into English

Background information

1. Brief description of the company (industry, customers, suppliers).
2. Description of the company's premises (environment, equipment, own/shared with other companies).
3. Number of employees.
4. What does information security mean to the company?
5. What kind of information does the company need for operation? What information is considered the most important?
6. Are there some functions which have been outsourced (for example cleaning, security, IT-facilities)?
7. Does the company have any information security related certificates (ISO 9001, ISO ISO 27001, ISO 18045, CMM, BSI, WebTrust, etc.)?
8. Have the values of the company been defined? Do the company values or documentation about them have any references to the values of information security (e.g. confidentiality, integrity, availability)?

Organizational security

9. Describe the information security policy of the company (goals, scope, is it documented). Are there other documents that are connected with information security (password policy, recruiting policy, travel instructions etc.)? When and why have the policies been made and by whom?
10. How are the information security roles and responsibilities divided into the different levels of organization or work roles? How are the responsibilities communicated to the employees? When are the responsibilities updated?
11. Are there any internal information security assessments in the organization? How often? Who carries out the assessments and how are they carried out?
12. Does the company monitor information security policy compliance? How?

Personnel security

13. Does the company cultivate employees' information security awareness (attitude and motivation toward information security)? How?
14. How are the personnel trained in information security issues? Are there any standard instructions or training material to new employees? If the personnel are not trained in information security issues, what are the most important reasons for not doing so?
15. Does the company perform any background checks on those people it recruits (criminal record, references, etc.)? How is the background check performed? What kind of risks does the company see in the recruiting process?
16. What kind of security statements or restrictions are there are in employment contracts or supplementary contracts? Why?
17. Do the employees have the possibility to telecommute (work at home)? What kind of instructions exist concerning telecommuting? Are there instructions on traveling?
18. Are there any documented or standardized procedures when an employment contract is terminated (access control, handing over work-related material, etc.)?

Software, hardware and network security

19. Do the employees have permission to install software on their workstations? Is it possible to install software even if it is forbidden? How is software maintenance organized in the company?
20. What portable media is allowed in the company (for example, USB memory sticks, CDs/DVDs)? Is the portable media protected against unauthorized access, misuse or editing? How? How is the use of portable media instructed?

21. Are the hard disks of laptops encrypted? If not, why? What kind of information is stored on laptops or mobile phones?
22. How is virus protection organized in the company (for example, updates, automatic scanning)?
23. What kinds of measures are used for protecting or encrypting telecommunications (for example, e-mail encryption programs, secure remote connections)? Is the use of telecommunications monitored in any way?
24. How is user authentication carried out when using remote connections?
25. Are employees using social media applications for work? Are they allowed to use these applications for personal communication at work? Are there any instructions concerning social media?

Physical security

26. Is there a physical access control system on the company premises? How are the access rights and restrictions defined? Is there any video surveillance on the premises?
27. Do the employees have identification cards? Are there temporary IDs for visitors? If not, how are the employees and visitors identified? Does the company have any instructions concerning visitors?
28. How is the access to the company's high security areas organized (for example server room, archives, other places which contain critical information)?
29. How is fire or water damage prevented, detected and alarmed?

Information assets security and access control

30. Does the company have a policy for access to information systems (for example, personal username and password)? On what grounds are access rights granted?
31. What is the password policy of the company? How is it monitored?
32. How is information classified (classification method, how the information should be treated, disposal, etc.)? Is the classification method documented?
33. Is the employees' access restricted only to the information they need to perform their work? Has the company paid attention to risky work combinations?
34. Do information and information systems have a named person who is responsible for them (the owner of the information/information system)? If there is no responsible person, describe substitute procedures.
35. What kind of backup policy does the company have? How is backup organized in practice? Where are the backups stored?

Business continuity planning and risk management

36. How are information security risks assessed in the company? Who assesses them and how often?
37. Describe the company's procedures to ensure business continuity in problem situations/accidents (for example, business continuity plan, plan to manage accidents, are there vice-employees to perform critical tasks or backup hardware). What happens if there is a fire in the company's premises?
38. Does the company have non-disclosure agreements with stakeholders? How is information exchange with partners organized? Has there been any information security related problems with partners? What kind of problems?
39. Does the company communicate its attitude toward information security to customers or suppliers? Is information security considered a marketing asset to the company? Could it be one in the future?