The *SMOL* Case: A SoDIS Approach to Teaching Electronic Transactions Security

Krassie Petrova & Rowena Sinclair,
Auckland University of Technology, New Zealand
kpetrova@aut.ac.nz, rsinclai@aut.ac.nz

Petrova, K. & Sinclair, R. (2007, Jun), The *SMOL* Case: A SoDIS Approach to Teaching Electronic Transactions Security. *Bulletin of Applied Computing and Information Technology* Vol. 5, Issue 1. ISSN 1176-4120. Retrieved from

1. INTRODUCTION

There is an increasing vulnerability of businesses to attacks on their systems, which has given rise to an increased interest in areas such as information security and risk management. In the project discussed here, the methodology developed for SoDIS (Software Development Impact Statement) was applied to evaluate risks related to business stakeholders, and to justify a security solution. A teaching case study was used. This report provides an update on the project, as presented at the 8th SoDIS Symposium (July 2006) in Wellington, New Zealand.

2. DISCUSSION

Students face a challenge when taught information security concepts, mostly due to the subject matter□s complexity coupled with its novelty and unfamiliarity. As a result they do not feel comfortable in applying what they have learnt in class to solve practical problems or even to use it as a reference in their further studies (Petrova, Kaskenpalo, Philpott, & Buchan, 2004). It was felt that SoDIS might provide a useful and practical framework to guide students in constructing their own knowledge and to build a bridge connecting the theory of information security and the practice of information security solutions (Boyle, 2000; Petrova, Sinclair, & Kwan, 2004).

2.1. Applying SoDIS

To enable the application of SoDIS to the teaching case, an overall framework of five premises was constructed based on findings and recommendations derived from literature reviewed (see for example Blakley, McDermott, & Geer, 2002; Hillier, 2003; Petrova & Sinclair, 2003; Petrova, Sinclair, & Kwan, 2004).

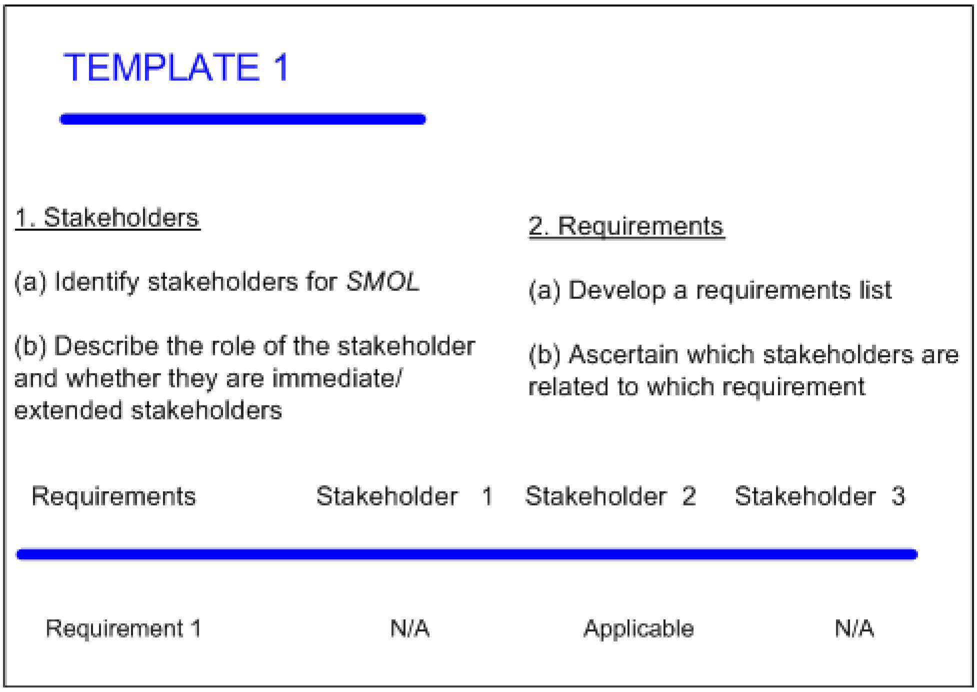
1. Use the specific subject area (□electronic transactions□) as the context
2. Use a case study (the □*SMOL*□ case - evolving around a SuperMarket *On*L*ine* business).
3. Assess student learning through a series of structured online learning activities (individual contributions, in class forum).
4. Assess student learning as they continue to contextualize the case (working in teams, in a team□s own work space).
5. Assess the final report (to include a SoDIS audit report).

Based on the framework above, a teaching and learning pilot experiment was conducted in Semester 1, 2006 at a New Zealand university. The class population included 55% Bachelor of Business students (majoring in Information Technology and/or eBusiness), 30% Bachelor of Computer and Information Sciences students, and 15% □other□ -

students taking the course as an elective component of their respective course of study.

2.2 Structured Online Activities

Students familiarized themselves with SoDIS independently and were asked to evaluate it in terms of usability and applicability to the case study; four templates were developed and provided to students to complete as part of their work on the case study (an example is shown in Figure 1).



TEMPLATE 1

1. Stakeholders

(a) Identify stakeholders for *SMOL*

(b) Describe the role of the stakeholder and whether they are immediate/ extended stakeholders

2. Requirements

(a) Develop a requirements list

(b) Ascertain which stakeholders are related to which requirement

Requirements	Stakeholder 1	Stakeholder 2	Stakeholder 3
Requirement 1	N/A	Applicable	N/A

Figure 1. A template to help students identify the business stakeholders

Student activities involved a SoDIS tutorial and product evaluation with regard to its usability and applicability to the *SMOL* case, and stakeholder and risk identification in several risk areas (system, knowledge management, electronic payment).

2.3 Results

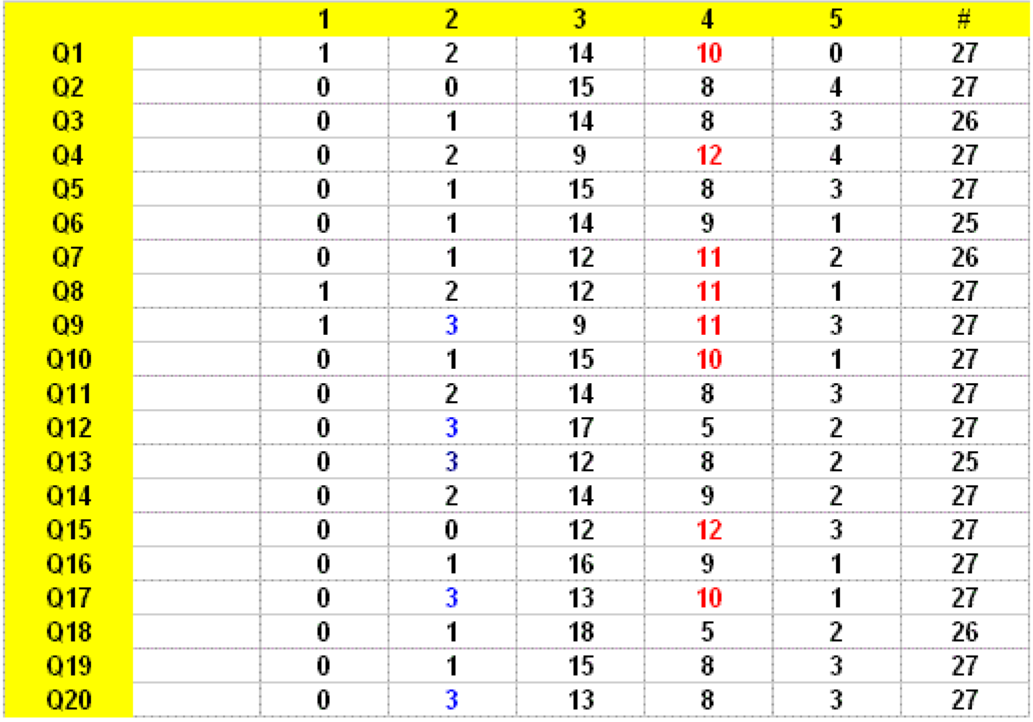
The overall academic results were very good, both for the semester and when compared to previous semesters: all students completed the course and passed, there was a good number of A grades (20% of all passes), and the average grade was 68% (a solid B grade). At the end of the course students were asked to self-evaluate the knowledge gained using a Likert scale from 1 (no knowledge gained) to 5 (expert knowledge gained) in twenty areas related to the course learning outcomes (Table 1).

Table 1. Areas where students were expected to acquire knowledge and expertise according to the course learning outcomes (adapted from Petrova & Claxton, 2007)

1. Investigating a business case	11. Understanding security standards
2. Identifying project stakeholders	12. Identifying security □problem areas□
3. Investigating stakeholders□ needs	13. Identifying ethical and privacy related risks

4. Understanding risk management	14. Identifying a security solution
5. Identifying risks related to stakeholders	15. Analyzing a security solution
6. Understanding information security techniques	16. Identifying an organization□s information security needs
7. Understanding disaster planning	17. Evaluating an information assurance solution
8. Understanding IT governance	18. Identifying systems information security requirements
9. Identifying on-line payment risks	19. Identifying users□ information security requirements
10. Identifying knowledge management risks	20. Evaluating information security products

The results obtained from 27 respondents (out of the 30 participants enrolled) are shown in Figure 2. Few students felt that they had become □experts□ by the end of the course □ however this result is in line with the attempt to keep the course at a relatively low beginners□ level. The good spread of □adequate□ (Likert scale 3) and □good□ (Likert scale 4) responses shows that students perceive themselves as having achieved a certain level of understanding of the basic concepts of information security requirements and solutions.



		1	2	3	4	5	#
Q1		1	2	14	10	0	27
Q2		0	0	15	8	4	27
Q3		0	1	14	8	3	26
Q4		0	2	9	12	4	27
Q5		0	1	15	8	3	27
Q6		0	1	14	9	1	25
Q7		0	1	12	11	2	26
Q8		1	2	12	11	1	27
Q9		1	3	9	11	3	27
Q10		0	1	15	10	1	27
Q11		0	2	14	8	3	27
Q12		0	3	17	5	2	27
Q13		0	3	12	8	2	25
Q14		0	2	14	9	2	27
Q15		0	0	12	12	3	27
Q16		0	1	16	9	1	27
Q17		0	3	13	10	1	27
Q18		0	1	18	5	2	26
Q19		0	1	15	8	3	27
Q20		0	3	13	8	3	27

Figure 2. Student self □evaluation results

2.4 Ongoing Work

In the coming semesters the authors will include a SoDIS audit report in the assessment and will continue to develop and improve the methodology described. A research model for studying student learning with SoDIS is under development and will be used to gather data in Semester 2 2006.

3. ACKNOWLEDGEMENTS

The authors would like to acknowledge the support and encouragement received from the participants in the 6th, 7th and 8th SoDIS symposia, the financial support in the form of a RELT grant from Auckland University of Technology which made the development of the course possible, and the enthusiasm and hard work of their students.

REFERENCES

Blakley, B., McDermott, E., & Geer, D. (2002). Information security is information risk management. *Proceedings of the ACM New Security Paradigms Workshop □01,* pp. 97-104.

Boyle T. (2000) Constructivism: A suitable pedagogy for Information and Computing Science? In Proceedings of the 1st Annual Conference of the LTSN Centre for Information and Computer Sciences, Heriot-Watt, Edinburg, UK.

Hillier, P. (2003, December). The role of ethics in information security. *ITAudit, 6.* Retrieved January 3, 2006 form http://www.theiia.org/ITAudit/index.cfm?act=itaudit.archive&fid=5466.

Petrova, K. & Claxton, G. (2007). Curriculum change and alignment with Industry: A student perspective. In G. Lowry & R. Turner (Eds.), Information systems and Technology education: From the university to the workplace.IDG Publishing, Hershey, PA, USA.

Petrova, K., Kaskenpalo, P., Philpott, A. & Buchan, J. (2004). Embedding information security curricula in existing programmes*. Proceedings of the 1st Annual Conference on Information Security Curriculum Development*, Kennesaw, GA, USA, pp. 20-29.

Petrova, K. & Sinclair, R. (2003). Expanding the understanding: Transactions and security awareness for eBusiness students. *Journal of Applied Computing and Information Technology, 7*(1), pp. 82-88.

Petrova, K., Sinclair, R., & Kwan, C.-T. (2004). Risk assurance for triple-bottom line reporting using SoDIS. In Cusack, B. (Ed.) *Proceedings of the 2004 IT Governance Conference*, Auckland, New Zealand, pp. 59-68