USING SOFT SYSTEMS METHODOLOGY TO FACILITATE THE DEVELOPMENT OF A COMPUTER SECURITY TEACHING MODULE

J. BIGGAM, A. HOGARTH

Department of Business Information Management, School of Business, Glasgow Caledonian University, Glasgow, SCOTLAND, UK

Telephone: (0141) 331 3943

Fax: (0141) 331 3193

E-Mail: J.Biggam@gcal.ac.uk, A.Hogarth@gcal.ac.uk

Key words: Computer Security, Computer Crime, Soft Systems Methodology, Requirements Engineering

Abstract: Computer security issues are now commonplace in the business community. Incidents such as computer viruses, Web vandalism, computer theft, etc. are regularly highlighted by the media. Indeed, the drive towards E-Business has raised the profile of security incidents. Many stakeholders play an important part in counteracting these security breaches, including law enforcement, the business community, hardware and software vendors, and researchers. The purpose of this paper is to highlight the role of universities in the battle against computer security breaches and to show, through a case study, how one university used the Soft Systems Methodology (SSM) to develop a computer security module for its undergraduate students.

telephoned a company to report a security vulnerability within the company's Web site, but rather than thank the student for highlighting this security issue, the company instead threatened legal action against the student. A recent survey (Computer Security Institute [4]) highlights that only 25% of respondents reported computer security issues to law enforcement,

In terms of gaining statistics, within Scotland there have been no surveys ascertaining the extent of computer crime. Although the police produce crime statistics, the fact that computer crime is not a legal term means that there are no police-produced computer crime statistics for Scotland.

Nevertheless, there are a number of reliable sources throughout the UK and abroad, that indicate the extent of computer security in general. Typical sources include the Audit Commission, the dti, and the Computer Security Institute. The aforementioned CSI 2000 Survey, actually highlights a decrease in computer crime. Examples of decreases include: Web vandalism (down from 98 incidents in 1999, to 64 incidents in 2000); Financial Fraud (27, 3); Denial of Service attacks (93, 60); and Theft of Transaction Information (25, 8).

This is not to be complacent. Although Business-to-Business transactions on the Web are now well established, there is a slow take-up of Business-to-Consumer transactions, the latter the result of customer fears over security (Aubrey-Jones [5]). The public perception, via media publicity, is playing a large part in the growth, or lack of it, in Business-to-Customer transactions. Previously, if a company suffered graffiti on its physical buildings, the impact to the public and the organization was minimal; but, place the same graffiti on a company's Website, and the impact can be immediate: Web business can be suspended to fix the security vulnerability and customer confidence on the organisation's ability to protect customer data suddenly becomes an issue. The result can be loss of business.

According to a report by the International Chamber of Commerce's Commercial Crime Services unit [6], 2,776 of the 4,139 cases referred to the chamber by its members were directly connected to crime, fraud or deliberate misrepresentation by website traders offering bogus goods or services. It is clear that computer crime, particularly with the advent of E-Business, is here to stay. That is not to adopt a defeatist attitude but, instead, an effort at facing reality so as to be better placed to tackle computer crime.

Although there are many stakeholders in the field of computer security (Biggam and Hogarth [7]) – business community, police, hardware/software

vendors, researchers, etc. - the purpose of this paper is to look at the role of universities in contributing towards the field of computer security and to show, specifically, how Soft Systems Methodology could be used to assist in the development of a computer security teaching module.

2. TACKLING COMPUTER SECURITY: A UNIVERSITY PERSPECTIVE

How can an organization tackle computer security? It is a simple matter to say that an organization ought to implement a standard such as BS7799, or hire consultants to implement a Firewall, but a key issue is how an organization can determine its initial security requirements (Biggam and Hogarth [8]).

There are many stakeholders involved in the field of computer security, including:

- Business community
- Police
- Perpetrator(s)
- Hardware/software vendors
- Researchers
- Users

Each of these stakeholders have different roles to play, but one stakeholder that ought to play a more active role, is the University. Universities often contribute in terms of important research (notable examples include London School of Economics and Leicester University), but it is in the teaching of computer security that universities ought to play a more active role.

Within Scotland, there are 13 universities:

1. University of Glasgow
2. University of Strathclyde
3. Glasgow Caledonian University
4. University of Paisley
5. University of Stirling
6. University of Edinburgh
7. Heriot-Watt University
8. Napier University
9. University of Dundee
10. Abertay University

11. University of Aberdeen
12. Robert Gordon University
13. St Andrew's University

In terms of teaching computer security, all of the above universities have some element of computer security within their teaching syllabus. However, it is interesting to note the context in which computer security is taught. All the universities teach computer security from a technical perspective, and so it is no surprise to see the subject taught within computer science, or equivalent, departments. Even then, though, computer security is not taught as a module in its own right, but rather as aspects of other modules (e.g. Systems Development, Computer Programming, etc.). There is a reasonable case that security ought to be integrated with other computing subjects (because business when they develop their computer systems, ought to integrate their security with their systems development process), but, equally, in terms of student learning, computer subjects are often separated (Computer Organization, Networks, Programming, Web Design, etc.).

It is also surprising not to find evidence of a computer security module within business-type departments in Scotland. The business community regularly suffers from security breaches, and so it makes sense to educate those who will work in that community to aid in the security of that environment. Although technical solutions to security problems are valued, it is the business case that determines whether or not security is treated seriously within an organization.

One of the universities – Glasgow Caledonian University (GCU) – attempted to address the issue of incorporating a computer security module within its School of Business. The following sections describe how GCU used the Soft Systems Methodology (SSM) to facilitate this development.

3. CAPTURING SECURITY REQUIREMENTS USING SSM

What is SSM and why is it suited to capturing computer security requirements? SSM was developed in the 1980s by Checkland [9] and Checkland and Scholes [10] to “enhance problem situations”. Where the system issues were clear-cut and well-defined, then the solution could be derived through a technical methodology, such as SSADM (Ashworth and Goodland [11]). Where the system issues were unclear or fuzzy, then SSM was recommended as a means of clarifying the problems. In other words,

SSM was not intended primarily as a means of producing technical solutions, but rather as a vehicle to facilitate the clarification of (softer) issues.

A simple perspective is to view system methodologies within two opposing camps: hard methodologies (such as SSADM) with their emphasis on technical solutions and soft methodologies (such as SSM) with their emphasis on people/organizational issues. However the reality is complicated, with methodologies ranging in various degrees between 'hard' and 'soft': Mumfords and Land's socio-technical approach, RAD, DSDM, JAD, etc. (Avison and Fitzgerald [12]; Hogarth and Biggam [13]).

SSM is a useful way to capture user requirements. SSM concentrates on stakeholder perspectives and thus facilitates user involvement. In addition, the tools used (CATWOE and Rich Pictures) are easy to employ and understand: this allows continued participation of user groups. The major benefit of SSM is the desire to move from "the problem unstructured" to "the problem structured" to "desirable changes".

This approach to systems analysis is well-suited to security issues: too often the technical solution is assumed (e.g. Firewall) without much thought given to user requirements or stakeholder perspectives. SSM would allow organizations to understand their security issues, clarify their security needs (including technical requirements) and so be better placed to protect their assets. It is interesting to note that ICL, through the use of their Business Impact Assessment methodology, adopt a 'soft' approach to ascertaining an organization's security requirements.

Users are an important group of stakeholders who have a critical role in the capture of user requirements. It ought to be emphasized that their value in the systems development process, particularly in the capture of user requirements, is not only recognized by Checkland but by researchers in other fields, e.g. computer security (Adam and Sasses [14]; Rannenberg [15]).

4. USING SSM TO ASCERTAIN TEACHING MODULE REQUIREMENTS: GLASGOW CALEDONIAN UNIVERSITY (GCU)

The following example illustrates how SSM could be used to capture user requirements. When the Division of Business Information Management (BIM) at GCU was interested in developing a computer security module for undergraduate students, SSM was used to clarify module requirements. The choice of SSM was based on two reasons: one, module issues were initially ill-defined; and two, SSM was known to the module leader, and so the exercise in using SSM, initially, was borne out of curiosity.

SSM has gone through various changes since its inception, but the SSM structure adopted for this exercise was:

Figure 2. SSM Structure

4.1 Stage 1: The Problem Situation Unstructured

There was a desire for additional undergraduate modules at undergraduate levels 3 and 4 (ordinary and honours, respectively) within the School of Business in general, and within the Division of Business Information Management (BIM) in particular. At the same time, a number of staff, with previous experience of teaching computer security within a

different department, but now residing in BIM, expressed an interest in developing a teaching module in computer security. Although BIM had taught some aspects of computer security to undergraduate students (e.g. backup procedures, the need for password control, etc), the delivery of a full module devoted to security was something new. As such, the initial module requirements were unclear and fuzzy.

Problem situation unstructured:

Figure 3. Rich Picture Element

4.2 Stage 2: The problem Situation Expressed

Two tools that are used in SSM to “enhance the problem situation” are CATWOE and Rich Pictures. Each aids in clarifying roles and issues. In the context of module development, the use of CATWOE resulted in the following listing:

- C Customers (i.e. beneficiaries of the ‘system’ i.e. module):
Students; BIM, School of Business; Business Community; Staff (in terms of staff development)
- A Actors (i.e. those who carry out essential activities in the module):
Module team; BIM (supplying resources); School of Business (in terms of validation and quality control); externals (academic and business); students (lectures/seminars/labs/assessments/feedback)
- T Transaction (i.e. change expected to take place):
Module idea – Module delivery
- W Weltanschauung (i.e. stakeholder perspectives): See Rich Picture
- O Owners (i.e. person/group to whom module team are responsible):
BIM (Subject Quality Group); School of Business
- E Environment (i.e. environment in which relevant system is placed):
Module resides in BIM, but offered to all Business students

The use of CATWOE helped identify the main stakeholders together with the target audience.

4.3 Stage 2: The Rich Picture

The Rich Picture produced was essentially a cartoon illustrating issues to be tackled to produce a successful module in computer security. This picture helped visualize a complex mess of interacting people, roles, threats, facts, observations, etc. Some of the elements of this Rich Picture are shown below:

Figure 4. BIM Rich Picture Element Expressing Staff Views

Figure 5. STUDENTS Rich Picture Element Expressing Student Views

The Rich Picture highlighted a number of issues, including:

- Rationale for a module in computer security
- Module content
- Resourcing (staff, supporting research, hardware, software, rooms)
- Student interests
- External support (academic and business)

Although there are existing module development processes used within BIM to facilitate module development and validation, the use of SSM assisted the module leader in clarifying module issues in a simple and straightforward manner. The use of Rich Pictures was particularly beneficial in visualizing non-technical issues.

4.4 Stage 3: Define the System under Investigation

Initially, this stage was viewed as less helpful than the previous stages. The ‘system’ as such was a teaching module, which, within the University environment, was clearly understood. However, what did materialize was the need to fit the module content within the context of a business environment, to reflect the principal teaching theme within BIM. Thus, “Computer Security” as a title was replaced with the title “Business Information Systems Security”.

4.5 Stage 4: Produce a Model of what you want the System to do.

This stage was interpreted as developing the actual module descriptor at an appropriate level for undergraduate students. The Learning Outcomes reflected industry concerns:

- Security Trends
- Security Life Cycle
- Risk Assessment
- Security approaches and standards (e.g. BS7799)
- Disaster Recovery
- Legal Issues (e.g. Computer Misuse Act 1990; Data Protection Act 1998)
- E-Business Security (e.g. PKI)
- Ethics
- Miscellaneous (e.g. Computer Forensics, Biometrics)

4.6 Stage 5: Compare Proposed Model (in Stage 4) with Rich Picture (in Stage 2) to determine if Problem Situation is Resolved

A number of problems were identified. Stage 2 highlighted the need for a module to meet the needs of business students, but the initial module descriptor was found to be too technical in nature, thus seen as inappropriate to business students. The module descriptor was then changed (but not in terms of subject headings) to reflect the subject content and target audience.

The assessment process was another key issue that was highlighted. The Rich Picture revealed one aspect of University thought, that new modules ought to consider new modes of module delivery and assessment:

Figure 6. UNIVERSITY Rich Picture Element Expressing University View

The module descriptor developed at stage 4 had not taken this on board. The traditional approach to teaching revolved around the lectures/labs/seminar model, and assessment was normally weighted towards end-of-semester examinations. The staff involved in the module delivery were concerned about making radical changes to the traditional teaching model and so retained the lecture format but made the seminars and labs student-centred. In terms of the assessment, it was decided to get the students to produce a mock conference paper (including abstract, etc.) for the coursework and to alter the traditional weighting between coursework and exam: 70% coursework (conference paper), 30% class test.

4.7 Stages 6 and 7: Identify Feasible Changes and Action Changes

The module was successfully validated and implemented in academic year 1999-2000, Semester B, to honours students in the School of Business. Student feedback, via standard university questionnaires, was overwhelmingly positive. The academic external praised the assessment. One criticism highlighted the need for software illustrating BS7799. This deficiency was corrected for the next academic year.

5. CONCLUSION

Computer security is a field worthy of academic study, not only in terms of research but within the context of teaching. However, there are difficulties introducing computer security in to the university curriculum as a subject in its own right:

- Who owns the module?

- How does it fit into the School/Faculty/Department/Division portfolio?
- Do the resources exist particularly with respect to staff expertise and research?
- Who is the target audience?
- What level ought it be aimed?
- and what should be the module content?

Using SSM is a simple and practical way to clarify some of these issues. Particularly useful is the easy-to-use tools CATWOE and Rich Pictures. An additional benefit of SSM, not initially realized in the case study, was that a straight-forward record of development was recorded, mostly of a visual nature (i.e. Rich Pictures), allowing a quick appreciation of the issues that were raised and tackled from inception to fruition.

Although SSM was used in this paper to facilitate the development of a computer security module appropriate to undergraduate students, the use of SSM is not restricted to module development. Perhaps organizations ought to consider using SSM as a front-end means of clarifying their security requirements.

6. REFERENCES

- [1] Biggam, J. (2001). 'Defining Knowledge: an Epistemological foundation for Knowledge Management', *Proceedings of the Thirty-Fourth Annual Hawaii International Conference on System Sciences*, IEEE, January 2001.
- [2] Gollmann, D. (2000). *Computer Security*, John Wiley & Sons, Cambridge.
- [3] Martin, B. (2001). 'Attrition' Web site: [Http://www.attrition.org/security](http://www.attrition.org/security)
- [4] Computer Security Institute (2000). 'Computer Security issues & Trends', CSI/FBI Survey, Vol VI No. 1, Spring 2000
- [5] Aubrey-Jones, D. (1999). 'Web Browser Security', *Proceedings of The 16th World Conference on Computer Security, Audit & Control*, Elsevier Advanced Technology.
- [6] Commercial Crime Services (2000). *Report on Computer Fraud*, International Chamber of Commerce, London.
- [7] Biggam, J. and Hogarth, A. (2000). 'Information Systems Security in the Age of Electronic Commerce', *Conference Proceedings of Management Information Systems 2000*, Lisbon, June.
- [8] Biggam, J. and Hogarth, A. (1996). The Development of a 'Computer Security Requirement Specification': Embedding and Merging ICL's 'Business Impact Model' with Soft Systems Methodology (SSM), *Proceedings of the 3rd BCS Information Systems Methodologies Specialist Group Conference*, University College Cork, Eire.
- [9] Checkland, P. B. (1981). *Systems Thinking: Systems Practice*. Wiley, Chichester.
- [10] Checkland, P. B. and Scholes, J. (1991). *Soft Systems Methodology in Action*. Wiley, Chichester.

- [11] Ashworth, C. and Goodland, M. (1990). *SSADM A Practical Approach*. McGraw-Hill International Series in Software Engineering, London.
- [12] Avison, D. E. and Fitzgerald, G. (1992). *Information Systems Development Methodologies, techniques and Tools*. Blackwell Scientific Publishing, Oxford.
- [13] Hogarth, A. and Biggam, J. (2000). 'The Social and Technical Effects of Introducing Groupware into the Educational Environment', *Proceedings of the ACM/OCG Conference on Educational Information and Communication Technology (EDICT 2000)*, Vienna.
- [14] Adams, A. and Sasse, M. A. (1999). 'Users are not the enemy: why users compromise security mechanisms and how to take remedial measures', *Communications of the ACM*, 42(12), pp.40-46.
- [15] Rannenbergh, K. (2000). 'Multilateral security – a concept and examples for balanced security', *Proceedings of the 9th ACM New Security Paradigms Workshop 2000*, September, Cork, Ireland, ACM Press.