December 2002

Developing a Postgraduate Course in Information Security: a confusion of terms

W. Hutchinson
Edith Cowan University

M. Warren
Deakin University

Developing a Postgraduate Course in Information Security: a confusion of terms

W Hutchinson[1] and M Warren[2]

[1]School of Computer and Information Science
Edith Cowan University
Mount Lawley, Western Australia
w.hutchinson@ecu.edu.au

[2]Department of Computing and Mathematics
Deakin University
Geelong, Victoria, Australia

Abstract

This paper examines problems with defining the requirements for a postgraduate course in Information Security. It examines the concept of information and from that develops the components needed for a comprehensive and integrated programme. Also, it examines the confusion associated with the term' Information Security'.

Keywords

Security training, information security, graduate programmes

INTRODUCTION

This paper originated from an idea to create a full postgraduate programme in Information Security. The university concerned already had a Graduate Certificate programme in Computer Security consisting of four units (Computer, Information, Database, and Computer Facilities Security) and a research Masters in Computer Security, which had four preliminary units (Computer, Database, Information, and Database Security). A number of unrelated elements stimulated the desire to produce a new course. The first was recognition, mostly by students, that the units tended to overlap in content. This was especially true of Computer and Information Security. The second factor related to the need for an increase in the development of information security professionals at all levels and the fact that this cannot be met using the existing education in most countries (Schou, 2001). The third was the intake of a number of staff who had research interests in Information Warfare (Denning, 1999; Waltz, 1998; Hutchinson and Warren, 2001a; 2001b).

This latter aspect led to a desire to develop a more inclusive Information Security course based on the concept of 'Information Warfare'. This was thought necessary to bring the education of Information Security out of the reactive and defensive paradigm found in many security courses. A unit in this subject had already been running in a Doctor of Business Administration programme. The idea was to expand on this concept and include all the aspects of information security. However, the initial problem was defining both 'information' and 'information security'. The former was a term used by various people to mean anything from straight computer security to military attacks on infrastructure. It was a broad expression that also included in some quarters (Campen and Dearth, 2000) such people-orient topics such as psychological warfare. In fact, Campen and Dearth would say that psychological warfare is the main aim of information warfare. It seemed that this broad expression would form the basis of the course. However, there was some concern over the name 'information warfare' as a full course. This concern was caused by a perception that the term was short-term fad, and also that others had (especially the military) used the term 'information operations' (a slightly different concept) for much the same subject material.

The term 'information security' cropped up again. It was amore conventional term and seemed to have a relatively distinct meaning. However, after searching texts and Information Security sites such as that of the Information Security Magazine (2002), it became clear that there was a massive overlap with conventional Computer Security. If fact, there was little to distinguish between them. The Australian Defence Signals Directorate (DSD, 2002) defines it thus:

> *Information security (Infosec) is usually defined as the combination of communications security (Comsec) and computer security (Compusec). The definition may also include radiation security (Radsec), which refers to emissions from devices such as monitors and printers (also known as TEMPEST). In short, the term Infosec relates to the security of any information that is stored, processed or transmitted in electronic or similar form.*

This is a totally technology and data based view. Only one text found (Pipkin, 2000) seemed to stray from this conventional viewpoint and actually attempt to talk about information rather than technology and data.

Therefore, a decision was made to go 'back to basics', and examine the word 'information'. The conventional definition of a data-information-knowledge-wisdom continuum did not prove very useful. Previous experience trying to define 'Knowledge Management' made the team realise that this model was likely to create superficial and ambiguous ideas. Another model was sought. The most promising model and the one eventually used and modified information was that created by Boisot (1998). His definition of 'information', 'data', and 'knowledge' seemed the most appropriate to use and expand for this exercise.

DEFINING 'INFORMATION'

In Boisot's model, data is associated with a ***thing***, and discriminates between different states of the thing it describes. It consists of attributes of the events or objects it describes. On the other hand, knowledge is an attribute of an ***agent***. Knowledge is a set of interacting mindsets about data activated by an event. Hence, in most circumstances the word 'agent' means a human being or a group of people. Information is the set of data filtered by the agent within the bounds of the knowledge held by the agent. It establishes a link between the agent and the data. Figure 1 illustrates the concept. This figure shows that information is produced by a human/group receiving data, and using a subset of that data dependent on the context in which it is received and the individual's/group's mindset/worldview.

Using this model developed above, the basic concepts of information security can be shown. Figure 1 also illustrates the main attack strategies pertinent to each of the elements in information production. It shows the nexus between Boisot's model and information security/warfare.

The vulnerability of each component can thus be seen to be:

Data

If the target of an attack is the data, a number of things can be done:

- **Deny access to data**: this can be achieved by attacks on hardware or systems containing the data or its collection, or deletion of data. As much data has a temporal dimension, it could also involve the delaying of access to data to the point at which it becomes useless. These attacks can range from denial of service to the deliberate withholding of data.
- **Disrupt or Destroy data**: this is similar to the above, but disruption can be caused to the system collecting and storing the data, or to that part of the system, which disseminates it. Destruction of the data can occur by physical destruction of the storage medium, or the data itself, so it becomes irrecoverable in the time needed to make it useful. Of course, it can be argued that data is never destroyed, just the medium on which it is stored.
- **Manipulation of data**: data can by added, deleted, or amended to give the attacker advantage. A person committing fraud would often use this method.
- **Steal data**: much corporate data is confidential and can also give competitive advantage. Theft of this data (and remember, theft of data can go unnoticed as the victim could still have it) might give insights into the workings of the attacked thereby giving the attacker a possible business, negotiation, or criminal advantage. Thus, the consequences are different from the other three attack

methods in that 'good' information is unwillingly shared with unauthorised people or systems.

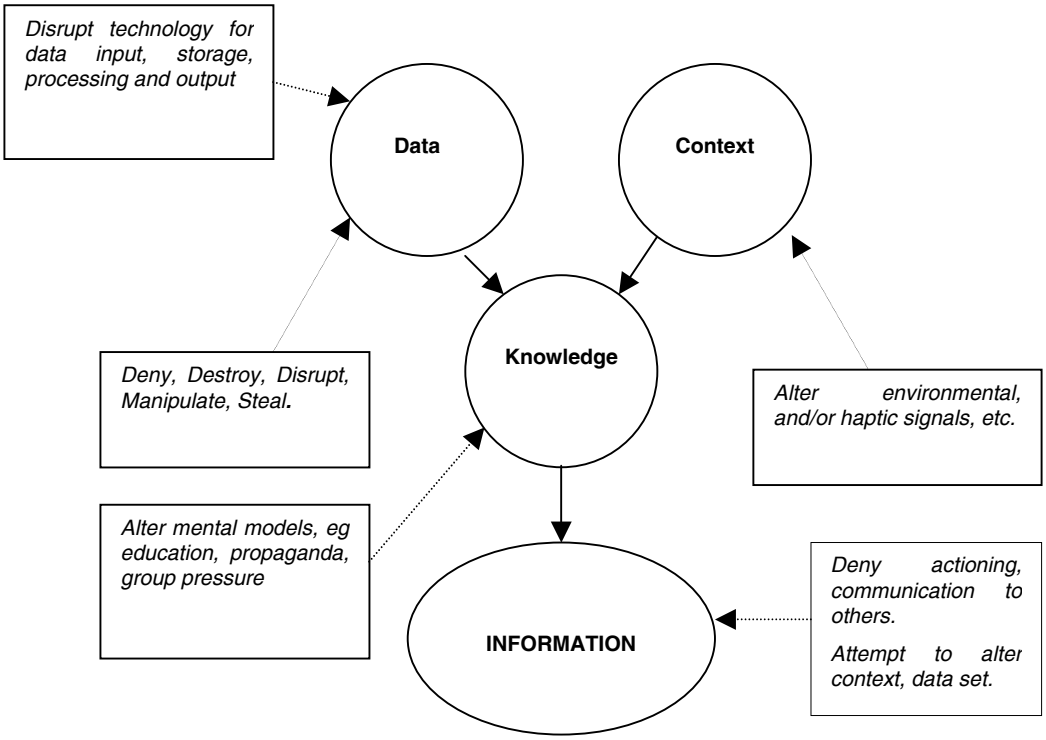

Figure 1: The relationships between data, context, knowledge, information; and the methods by which each element can be attacked (adapted from Hutchinson and Warren, 2001b)

Context

The objective in altering the context of a situation is that the target will misinterpret the data being presented. This can be achieved by affecting environmental or sensory signals received by the target in any particular situation. It is similar to an attack on data but is more ephemeral. In attacking context, you are trying to alter the situation in which the data is viewed. This can include such things as place, sensory surroundings, mood, and political climate. It is really concerned with manipulating the way the data are to be interpreted.

Knowledge

The strategies to deal with knowledge tend to be more long term**.** As mental models are developed by a person's experiences, they are created by education, social interaction, emotions, and so on. Changing perceptions is directed more toward the people themselves, and their thought processes. This can include public relations, advertising, and incentives. The assumption is that the attacker will **exploit** any situation created by the attack. This emphasises the need to defend human as well as technological assets as a part of an information security plan, something often ignored.

Information

Although information is now 'created', its dissemination can now be corrupted, stopped, or slowed.

It became increasingly obvious that a comprehensive course in Information Security would involve more than traditional computer security. Such a course would need elements that included:

- Defensive measures for data production/access/alteration/storage/destruction, data communication, knowledge management, data interpretation, information use and communication, and

- Offensive measures to utilise data/knowledge/information for organisational benefit.

It became increasingly obvious that a comprehensive course in 'Information Security' would involve more than a traditional computer security.

DESIGNING THE COURSE

The breadth of course and the need for inputs from various disciplines become apparent; see Figure 2.

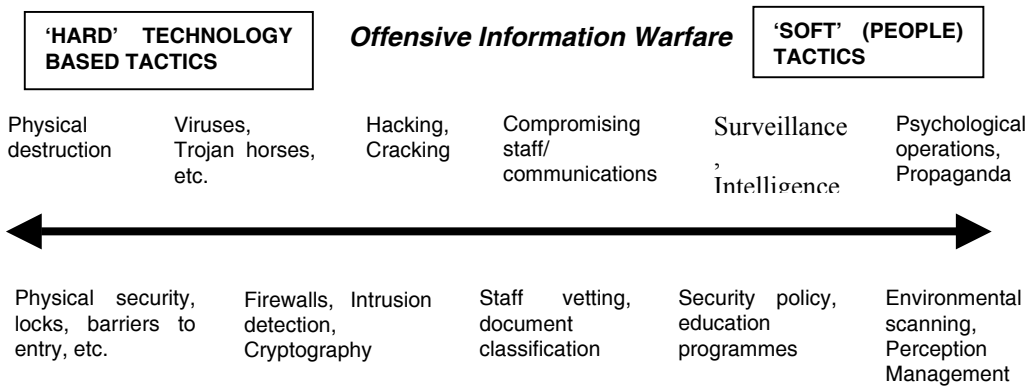

Figure 2: Examples of the range of topics needed in a comprehensive Information Security/Warfare course

It has to be admitted that as an advanced post graduate course, more attention was put into the course content and desired outcomes than the means of teaching this material. It was thought correctly or incorrectly that as a postgraduate course, it should be knowledge focused rather than concentrating on the educational techniques needed.

The discipline area was separated into 'soft' (people oriented) and 'hard' (technology oriented) components as implied by the Boisot model. The more generic skills required from all students were then determined to enable these to be integrated into the units. These included skills based on logic, analysis, induction, deduction, observation, cultural and personality appreciation, and lateral thinking. Much of this is achieved by such exercises as scenario, role-playing, and analytical problem solving. It was felt that these skills were an essential part as defensive and offensive require two separate, complementary mindsets; in fact, two modes of thought. One protective, suspicious, conservative, and cautious; the other inventive, risk taking, aggressive. Both views are needed to exploit and protect the information assets within an organisation.

The subject content was then analysed. It needed to include the full breath for all students with the option for students to specialise in the 'soft' or 'hard' areas, or in fact, to generalise in both. Referring to the modified Boisot model in Figure 1, it needed to cover the elements of data, knowledge, context, and information protection and exploitation. As the investigation went on, some of the content included much of what is included in a conventional course in Intelligence (see LEIU, 2000 for a basic summary of an intelligence course). In fact, the nature of Information Security was changing to include both defensive and proactive (aggressive) elements resembling security (relatively passive protection), intelligence (active use of information), and counter-intelligence (aggressive protection of information and its resources). In fact, we were drifting very much into the Information Warfare/Intelligence paradigm. Recognising this, the course was renamed to Information Security and Intelligence.

Details of content needed to cover the full breadth of the area was established and spilt into domain areas. The core units were designed to cover the core body of knowledge. It should be noted that, in this context, a unit is a component (sub course) of a complete course. The final course is now being offered and is split into three stages:

Stage 1: Graduate Certificate

This consists of four units: 2 compulsory core units and two electives. This stage was designed to cover the full gambit of factors the Boisot model (the two compulsory units, plus two specialist units covering an element of the model. These are basically split into technological 'hard' units such as 'Network Security', 'Computer Security', or 'soft' human oriented units such as 'Media and Nation', or 'Global Communications'. The two compulsory units are:

- **Information Security:** a general introductory unit on Information Security principles, concentrating on protective measures. It covers all the elements in the Boisot model and both hard and soft areas from the defensive side.
- **Information warfare:** a general introduction to the more aggressive aspects of Information Security, including Offensive and Defensive Information Warfare but primarily the offensive. As above, it is a general unit that covers both hard and soft factors.

Stage 2: Graduate Diploma

This consists of three core and compulsory units. These cover advanced topics in the defensive mode (Information Security), advanced soft topics concerned with the mind/information interface (Perception Management), and the exploitation of information within an organisation (Contemporary Intelligence). The units are:

- **Perception Management**: a 'soft' unit, which covers psychological warfare. It is this unit that examines the aggressive use of information. Very much about the data/ knowledge/ context interface.
- **Contemporary Intelligence**: a 'soft/hard' unit, which examines contemporary intelligence and counter-intelligence practice. This is about the proactive use and defence of information. It involves all elements of the Boisot model but has emphasis in the Information realm.
- **Information Security:** a 'technology/ soft' base unit, which follows on from the earlier unit. It tends to stay inside the defensive mode but does show the interface between that and the offensive mode.

This stage provides the core of the course, whilst the former units are introductory in nature.

Stage 3: Masters

This stage consists of three units. There are two options:

- **Research/ Project:** a research project based either from the student's employment, or a theoretical based minor thesis, or
- **Three advanced units:** these can be chosen from a narrow selection of units from computer/ network/physical security, ethics, cybercrime, or media based units

This final stage allows the student to specialise by taking advanced units, or to examine their own organisation using the skills developed in the earlier parts of the course, or to research a topic of interest in the field.

The course still covers traditional fundamental security principles (such as confidentiality, integrity, and availability) and in the technical computer security based units deals with those basic topics defined by White *el al*. (1999) as:

- Risk analysis
- Authentication
- Access controls
- Basic principles of cryptography
- Knowledge of the types of malicious software that exist;
- Basic network security (including a discussion of web security).

Within the non-traditional security units (for example Information Warfare), a more innovative way has to be used to teach the subject. The School has been involved with the Australian Department of Defence in running Information Warfare exercises involving Australia, Canada, NATO, New Zealand, United Kingdom and USA using collaborative learning (war gaming) environments (Davey, 2001). This has led to an understanding that newer more innovative teaching methods may have to be applied to teach certain key concepts.

In this course the progression of units is thought to accomplish the difficult task of covering the body of knowledge required in this ill-defined field, moving away from the traditional defensive security norm.

THE STATE OF SECURITY EDUCATION AND R&D WITHIN AUSTRALIA

The course described also has a larger impact; it helps Australia and its future development. The Australian Federal Government department NOIE (National Office of the Information Economy) had been looking at the IT security situation within Australia. The aim of the project was to determine what the situation was within Australia in regards to IT Security education. The project found that the main requirements were (Aeuckens, 2001):

1. Demand for people with security skills is expected to be strong over the few years.
2. Recruitment of personnel with security skills is difficult compared to other IT&T skills.

The project also identified some key issues that related to Australian organisations and the impact of security, these key issues were (Aeuckens, 2001):

- *Demand is rising* - ◘As security becomes an integral business issue, demand for skilled personnel is growing within Australia;
- *Recruitment of people with the right skill sets is difficult* - ◘The greatest difficulty is in recruiting people with well-rounded security and risk management skills (likely to include technical and business skills);
- *Security is not just an issue for security personnel* - ◘All IT personnel should have an awareness of security issues and their place in a business environment;
- *Limited Graduate programs* - ◘Many organisations recruited new IT graduates. Graduates did not generally have any specific understanding of security, therefore it was necessary for them to undergo further training;
- *Education and training opportunities in e-security are not widely available* - ◘The minimum qualification demanded by employers is generally at the Bachelor level but tends to lack security expertise.

A further NOIE investigation was into security research and development within Australia. The NOIE research project found it was essential to ensure the long-term health of Australia's E-security research for a number of reasons. (King, 2001):

- Dependence on foreign e-security providers limits the input that Australia has into the type and character of products and services developed. Australia should not be reliant upon other countries dictating appropriate levels of security;
- A commercial imperative also exists. A secure and trusted electronic environment is a necessary condition enabling electronic commerce;
- The e-Security industry is experiencing substantial growth. R&D is an important link in the innovation chain driving developments in this industry sector. The Government has an important role to play ensuring that Australia is a global supplier as well as a consumer of e-security products and services. Eventually, some kind of security technology, be it hardware or software, will be resident in every networked device. Maintaining a critical mass of e-security R&D in Australia is essential to achieving this aim;
- A robust e-security R&D environment can also play a key role in attracting skilled e-security workers to Australia, and keep home grown talent from moving overseas;

- E-Security R&D will assist in providing the Government with the tools to perform its role in law enforcement activities to protect information infrastructure and the public.

The course described within the paper as well as the joint research undertaken by the authors symbolises the steps that have to be taken to resolve the problems defined by the Australian Federal Government. Australia faces a common problem with many countries within the developed world. It is that there is limited teaching of security skills within Australian Universities and a flawed approach to security R&D within Australia. These two facets have to be considered as a whole, as this defines the IT Security culture of Australia within the new millennium, but raising awareness across the economy of the importance of e-security is seen as a major priority (NOIE, 2001).

CONCLUSION

The exercise of developing this course better focused the participants' thoughts on an area in which they were 'experts'. Hopefully, the end product is a comprehensive addition to the education world, and will add to intellectual progress in this area. It does expose the narrow, technological bias of many security courses. Perhaps, this view reflects the general impression in the IT industry that data and technology are synonymous with information. The development of this course shows that information security is, in fact, a much richer area of study and research.

REFERENCES

Aeuckens D (2001) E-Security Skills, Education and Training in Australia: A Policy Scoping Paper, NOIE Report. Canberra, Australia

Boisot, M.H. (1998) Knowledge Assets. Oxford University Press, Oxford.

Campen, A.D., Dearth, D.H. (eds) (2000) CyberWar 3.0,: Human Factors in Information Operations and Future Conflict, AFCEA International Press, Fairfax, Virginia.

Davey J (2001) Information Warfare and Cyber warfare: More Than Just Software, Proceedings of the IFIP TC11 WG 11.8 Second World Conference on Information Security Education, 12-14 July, Perth, Australia. 101-112

Denning, D.E. (1999). Information Warfare and Security, Addison Wesley, Reading: Mass.

DSD (2002) What is InfoSec? URL: http://www.dsd.gov.au/infosec/ Accessed 12 May 2002.

Hutchinson, W.E., Warren, M.J. (2001a) Information Warfare: Corporate Attack and Defence in the Digital Age, Butterworth-Heineman, Oxford.

Hutchinson, W., Warren, M. (2001b) Principles of Information Warfare, Journal of Information Warfare, **1**,1: 1-6.

Information Security Magazine (2002) URL: http://www.infosecuritymag.com/ Accessed 25 Jan 2002.

LEIU(2000) Intelligence 2000:Revising the Basic Elements, LEIU/IALEIA, California Department of Justice.

King G. (2001) Report on e-security R&D in Australia: an initial assessment, NOIE Report. Canberra, Australia.

NOIE (2001). Protection of Australia's National Information Infrastructure & E-security Policy (Administrative and Operational Arrangements), Canberra, Australia.

Pipkin, D.L., (2000) Information Security: Protecting the Global Enterprise, First Edition, Prentice-Hall, Okalahoma, USA

Schou, C, (2001) Information Security Education – A Worldwide Workforce Crisis, Proceedings of the IFIP TC11 WG 11.8 Second World Conference on Information Security Education, 12-14 July, Perth, Australia. 101-112

Waltz, E. (1998) Information Warfare – Principles and Operations. Artech House, Norwood.

White G, Marti W, and Huson M (1999) Incorporating Security Issues Throughout the Computer Science Curriculum, Proceedings of the IFIP TC11 WG 11.8 First World Conference on Information Security Education, 17-19 June, Kista, Sweden. 19-26

COPYRIGHT