INFORMATION SECURITY MANAGEMENT, EDUCATION AND PRIVACY
IFIP – The International Federation for Information Processing

IFIP was founded in 1960 under the auspices of UNESCO, following the First World Computer Congress held in Paris the previous year. An umbrella organization for societies working in information processing, IFIP’s aim is two-fold: to support information processing within its member countries and to encourage technology transfer to developing nations. As its mission statement clearly states,

IFIP’s mission is to be the leading, truly international, apolitical organization which encourages and assists in the development, exploitation and application of information technology for the benefit of all people.

IFIP is a non-profitmaking organization, run almost solely by 2500 volunteers. It operates through a number of technical committees, which organize events and publications. IFIP’s events range from an international congress to local seminars, but the most important are:

- The IFIP World Computer Congress, held every second year;
- Open conferences;
- Working conferences.

The flagship event is the IFIP World Computer Congress, at which both invited and contributed papers are presented. Contributed papers are rigorously refereed and the rejection rate is high.

As with the Congress, participation in the open conferences is open to all and papers may be invited or submitted. Again, submitted papers are stringently refereed.

The working conferences are structured differently. They are usually run by a working group and attendance is small and by invitation only. Their purpose is to create an atmosphere conducive to innovation and development. Refereeing is less rigorous and papers are subjected to extensive group discussion.

Publications arising from IFIP events vary. The papers presented at the IFIP World Computer Congress and at open conferences are published as conference proceedings, while the results of the working conferences are often published as collections of selected and edited papers.

Any national society whose primary activity is in information may apply to become a full member of IFIP, although full membership is restricted to one society per country. Full members are entitled to vote at the annual General Assembly. National societies preferring a less committed involvement may apply for associate or corresponding membership. Associate members enjoy the same benefits as full members, but without voting rights. Corresponding members are not represented in IFIP bodies. Affiliated membership is open to non-national societies, and individual and honorary membership schemes are also offered.
INFORMATION SECURITY MANAGEMENT, EDUCATION AND PRIVACY

IFIP 18th World Computer Congress
TC11 19th International Information Security Workshops
22–27 August 2004
Toulouse, France

Edited by

Yves Deswarte
LAAS-CNRS, France

Frédéric Cuppens
ENST-Bretagne, France

Sushil Jajodia
George Mason University, USA

Lingyu Wang
George Mason University, USA

KLUWER ACADEMIC PUBLISHERS
NEW YORK, BOSTON, DORDRECHT, LONDON, MOSCOW
Contents

<table>
<thead>
<tr>
<th>Part</th>
<th>Title</th>
<th>Authors</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preface</td>
<td>ix 10th IFIP WG 11.1 Annual Working Conference on Information Security Management Program Committees</td>
<td>J.V. NIEKERK, R.V. SOLMS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IFIP TC11 WG 11.8 – Information Security Education Workshop Program Committees</td>
<td>K.L. THOMSONA AND R. VON SOLMS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>I-NetSec04 3rd Working Conference on Privacy and Anonymity in Networked and Distributed Systems Program Committees</td>
<td>T.B. BUSUTTIL, M.J. WARREN</td>
<td></td>
</tr>
</tbody>
</table>

PART ONE: 10th IFIP WG 11.1 Annual Working Conference on Information Security Management

- Corporate Information Security Education: Is Outcomes Based Education the Solution?  
  J.V. NIEKERK, R.V. SOLMS  
  3

- Towards Corporate Information Security Obedience  
  K.L. THOMSONA AND R. VON SOLMS  
  19

- CIIP-RAM - A Security Risk Analysis Methodology for Critical Information Infrastructure Protection  
  T.B. BUSUTTIL, M.J. WARREN  
  33
A Framework For Role-based Monitoring of Insider Misuse
A.H. PHYO, S.M. FURNELL, F. PORTILLA 51

Update/Patch Management Systems: A Protocol Taxonomy with Security Implications
A. COLARIK, C. THOMBORSON, L. JANCZEWSKI 67

Investigating a Smart Technology
K. O’SULLIVAN, K. NEVILLE, C. HEAVIN 81

PART TWO: IFIP TC11 WG 11.8 – Information Security Education Workshop

Laboratory Support for Information Security Education
N. MILOSLAVSKAIA, A. TOLSTOI, D. USHAKOV 101

An Holistic Approach to an International Doctoral Program
L. YNGSTRÖM 117

A New Paradigm for Information Security Education at Doctoral Level
N. JAYARATNA 133

Highly Qualified Information Security Personnel Training in Russia
V. GORBATOV, A. MALUK, N MILOSLAVSKAYA, A. TOLSTOI 141

Doctor of Philosophy: IT Security
J. SLAY 147

Doctoral Programme on Information and Communication Systems Security at the University of the Aegean
S. KATSIKAS 153

An International Security Perspective
G. QUIRCHMAYR 159

Do Military Forces Need Ph.D.s?
R. DODGE 165
A Doctoral Program with Specialization in Information Security:
A High Assurance Constructive Security Approach
C. IRVINE, T. LEVIN

PART THREE: I-NetSec04 3rd Working Conference on Privacy and Anonymity in Networked and Distributed Systems

A Security Model for Anonymous Credential Systems
A. PASHALIDIS, C.J. MITCHELL

Private Information Storage with Logarithm-Space Secure Hardware
A. ILIEV, S. SMITH

Taxonomy of Mixes and Dummy Traffic
C. DIAZ, B. PRENEEL

Identity Management for Self-Portrayal
T. BAIER, C.P. KUNZE

Privacy Preserving Online Reputation Systems
M. VOSS

A Risk Driven Approach to Designing Privacy Enhanced Secure
E.V. HERREWEGHEN

Privacy Invasive Software in File-Sharing Tools
A. JACOBSSON, M. BOLDT, B. CARLSSON

Infusing Privacy Norms in DRM – Incentives and Perspectives
A. CAMERON
Preface

This volume gathers the papers presented at three workshops that are embedded in the IFIP/Sec Conference in 2004, to enlighten specific topics that are currently particularly active in Security.

The first one is the 10th IFIP Annual Working Conference on Information Security Management. It is organized by the IFIP WG 11.1, which is itself dedicated to Information Security Management, i.e., not only to the practical implementation of new security technology issued from recent research and development, but also and mostly to the improvement of security practice in all organizations, from multinational corporations to small enterprises. Methods and techniques are developed to increase personal awareness and education in security, analyze and manage risks, identify security policies, evaluate and certify products, processes and systems. Matt Warren, from Deakin University, Australia, who is the current Chair of WG 11.1, acted as the Program Chair.

The second workshop is organized by the IFIP WG 11.8, dedicated to Information Security Education. This workshop is a follow-up of three issues of the World Conference on Information Security Education (WISE) that were also organized by WG 11.8. The first WISE was organized by Louise Yngstrom in 1999 in Stockholm, and the next one, WISE’4, will be held in Moscow, Russia, 18-20 May 2005. This year, the workshop is aimed at developing a first draft of an international doctorate program allowing a specialization in IT Security. The draft will be based upon both selected papers from individuals or groups (from academic, military and government organizations), and discussions at the workshop. This draft will be further
refined and eventually published as an IFIP Report. The Program Committee was chaired by Helen Armstrong, from Curtin University, Australia, who is also the Chair of the IFIP WG 11.8.

Finally, the last workshop is the 3rd Working Conference on Privacy and Anonymity in Networked and Distributed Systems (I-NetSec04), organized by the IFIP WG 11.4 on Network Security. The purpose of the workshop is to bring together privacy and anonymity experts from around the world to discuss recent advances and new perspectives on these topics, that are increasingly important aspects in electronic services, especially in advanced distributed applications, such as m-commerce, agent-based systems, P2P, etc. The Program Committee was co-chaired by Bart De Decker, from the Catholic University of Leuven, Belgium, who is also chairing the IFIP WG 11.4, and by Els Van Herreweghen, from IBM Research Lab, Zurich, Switzerland.

The carefully selected papers gathered in this volume show the richness of the information security domain, as well as the liveliness of the working groups cooperating in the IFIP TC-11 on Security and Protection in Information Processing Systems.

**Yves Deswarte**
General Chair
10th IFIP WG 11.1
Annual Working Conference on
Information Security Management
Program Committees

Program Committee Chair
Matt Warren, Deakin University, Australia

Program Committee
William Hutchinson, Edith Cowan University, Australia
Steven Furnell, Plymouth University, UK
Jill Slay, University of South Australia, Australia
Craig Valli, Edith Cowan University, Australia
Rossouw von Solms, Port Elizabeth Technikon, South Africa
Information Security Education Workshop
Program Committees

Program Committee Chair
Helen Armstrong, Curtin University, Australia

Program Committee
Colin Armstrong, Curtin University, Australia
William Caelli, Queensland University of Technology, Australia
Steven Furnell, Plymouth University, UK
Simone Fischer-Hubner, Karlstad University, Sweden
William Hutchinson, Edith Cowan University, Australia
Cynthia Irvine, Naval Postgraduate School, Monterey, CA, USA
Sokratis Katsikas, University of the Aegean, Greece
Natalia Miloslavskaia, Moscow State Engineering Physics Institute, Russia
Gerard Quirchmayr, University of Vienna, Austria
Corey Schou, Idaho State University, USA
Jill Slay, University of South Australia, Australia
Matthew Warren, Deakin University, Australia
Louise Yngstrom, Stockholm University, Sweden
I-NetSec04 – 3rd Working Conference on Privacy and Anonymity in Networked and Distributed Systems
Program Committees

Program Committee Co-chairs
B. De Decker, K.U.Leuven, Belgium
E. Van Herreweghen, IBM Research Lab, Zurich, Switzerland

Program Committee
S. De Capitani, Univ. of Brescia, Italy
Y. Deswarte, LAAS-CNRS, Toulouse, France
H. Federrath, Univ. of Regensburg, Germany
S. Fischer-Hübner, Karlstad Univ., Sweden
U. Gattiker, EICAR, Aalborg Univ., Denmark
K. Martin, Royal Holloway, Univ. London, UK
R. Molva, Eurécom, France
K. Rannenberg, Goethe Univ. of Frankfurt, Germany
P. Ryan, Univ. of Newcastle, UK
P. Samarati, Univ. of Milan, Italy
V. Shmatikov, SRI International, USA
PART ONE

10TH IFIP WG 11.1 ANNUAL WORKING CONFERENCE ON INFORMATION SECURITY MANAGEMENT
CORPORATE INFORMATION SECURITY
EDUCATION:
Is Outcomes Based Education the Solution?

Johan Van Niekerk ¹ And Rossouw Von Solms ²
Department of Business Information Systems, Port Elizabeth Technikon ¹; Department of Information Technology, Port Elizabeth Technikon ²

Abstract: Today’s global economy is increasingly dependent on the creation, management, and distribution of information resources. Information and its use permeate all aspects of modern society. Most modern organizations need information systems to survive and prosper. Information has become a valuable commodity and as such needs to be protected. This protection is typically implemented in the form of various security controls. In order for these controls to be effective, the users in the organization need to be educated regarding these controls. Recent studies have indicated that current user education programs fail to pay adequate attention to behavioral theories. This paper examines the educational principles an information security user education program should adhere to. It then introduces outcomes based education (OBE) and finally argues that OBE is ideally suited for the needs of information security.

Keywords: Information Security, Information Security Culture, Outcomes Based Education, Awareness

1. INTRODUCTION

In today’s business world, information is a valuable commodity and as such, needs to be protected. Information affects all aspects of today’s businesses, from top management right down to the operational level (Turban, et al., 2002. pp 3-37). In order to avoid loss or damage to this valuable resource, companies need to be serious about protecting their information. This protection is typically implemented in the form of various security controls (Barnard & Von Solms, 2000). However, it is very difficult
to know exactly which controls would be required in order to guarantee an acceptable minimum level of security. Furthermore, managing these controls to see that they are always up to date and implemented uniformly throughout the organization is a constant headache to organizations.

When selecting the controls to implement in an organization, it is important to refer to accepted international standards (Von Solms, 1999). There exist several internationally accepted standards and codes of practice to assist organizations in the implementation and management of an organizational information security strategy. Some of the better known examples would include the ISO/IEC 17799 (British Standards Institute (BSI), 1999) and ISO/IEC 13335 also known as GMITS (Guidelines to the Management of Information Technology Security (GMITS), 1995).

These standards and codes of practice provide organizations with guidelines specifying how the problem of managing information security should be approached (Von Solms, 1999). One of the primary controls identified by many of the major IT security standards published to date is the introduction of a corporate information security awareness program (BSI, 1999; GMITS, 1995). The purpose of such a program is to educate the users about information security or, more specifically, to educate users about the individual roles they should play in the effective execution and maintenance of these controls. Most security controls, whether physical, technical, managerial or administrative in nature, requires some form of human involvement. This paper will examine this dependence of information security on human involvement with specific emphasis on the role user education has to play in a corporate information security strategy. It will then propose outcomes based education (OBE) as a pedagogical methodology suitable for the information security education needs of organizations.

2. THE HUMAN SIDE OF INFORMATION SECURITY

Information security controls can generally be sub-divided into three categories: Physical controls, Technical controls and Operational controls (Thomson, 1998, p. 29). Physical controls deal with the physical aspects of security, for example; the lock on the door of an office containing sensitive documents. Technical controls are controls of a technical nature, usually software based, for example; forcing a user to authenticate with a unique username and password before allowing the user to access the operating system. The third category, operational controls, collectively including
business-, administrative-, managerial-, and procedural controls, consist of all controls that deal with human behavior in one form or another. These controls would include those that deal with the creation of information security policies and procedures, and administration of other controls. Both physical and technical controls, even though they do not deal directly with operational issues, usually require some form of human involvement. In an organizational context, these controls would thus have to be supported by procedures outlining the employee’s involvement in the use of these controls.

Employees, whether intentionally or through negligence, often due to a lack of knowledge, are the greatest threat to information security (Thomson, 1998, p. 12, Mitnick & Simon, 2002, p. 3). Operational controls rely on human behavior. This means that these controls are arguably some of the weakest links in information security. Unfortunately, both physical and technical controls rely to some extent on these operational controls for effectiveness. As an example, an operational control might state that a user leaving his/her office must logoff from the operating system and lock his/her office door. If a user were to ignore this procedure, both the technical control forcing authentication and the physical control of having a lock on the door would be rendered useless. Thus, anyone who thinks that security products, i.e. technical and physical controls, alone, offer true security is settling for the illusion of security (Mitnick & Simon, 2002, p. 4).

Siponen (2001) describes this tendency of organizations to settle for the illusion of security as a general human tendency to often blindly ignore complications in IT related issues. Without an adequate level of user cooperation and knowledge, many security techniques are liable to be misused or misinterpreted by users. This may result in even an adequate security measure becoming inadequate (Siponen, 2001) Organizations cannot protect the integrity, confidentiality, and availability of information in today’s highly networked systems environment without ensuring that each person involved understands his/her roles and responsibilities and is adequately trained to perform them (National Institute of Standards and Technology (NIST), 1998, p. 3).

Teaching employees their roles and responsibilities relating to information security requires the investment of company resources in a user education program. However, budgetary requirements for security education and training are generally not a top priority for organizations (Nosworthy, 2000). Organizations often spend most their information security budget on technical controls and fail to realize that a successful information security
management program requires a balance of technical and business controls (Nosworthy, 2000). Business controls in this sense refer to operational controls. According to Dhillon (1999), increasing awareness of security issues is the most cost-effective control that an organization can implement. However, in order to ensure that the maximum return on investment is gained, special care should be taken to ensure the success of the user education programs used. For educational programs this would mean ensuring adherence to proper pedagogical principles when these educational programs are compiled.

Most current user education programs fail to pay adequate attention to behavioral theories (Siponen, 2001). The emphasis of user education programs should be to build an organizational sub-culture of security awareness, by instilling the aspects of information security in every employee as a natural way of performing his or her daily job (Von Solms, 2000). Recent studies have indicated that the establishment of an information security “culture” in the organization is desirable for effective information security (Von Solms, 2000). Such a culture should support all business activities in such a way that information security becomes a natural aspect in the daily activities of every employee (Schlienger & Teufel, 2003). A detailed examination of how such a culture could be established in an organization falls outside the scope of this paper. Instead this paper will focus only on user education, one of the cornerstones required for the establishment of such a culture. For more information on the establishment of such a culture see e.g. (Van Niekerk & Von Solms, 2003; Schlienger & Teufel, 2003).

3. ELEMENTS OF INFORMATION SECURITY EDUCATION

The user education programs needed for information security purposes differ from traditional educational programs. Unlike traditional educational programs, these programs will primarily be aimed at teaching adults. Adults have well established, not formative, values, beliefs, and opinions (NIST, 1998, p. 20). The educational methodology used should thus be suitable for adult education. Furthermore, there are several other requirements specific to the role that such a program will play in the overall organization’s information security efforts. In the following sections, this paper will suggest and attempt to motivate some of the features that should typically constitute such an information security education program.
3.1 Everyone should be able to “pass” the course.

Nosworthy (2000) states that each person in the organization from the CEO to House Keeping staff must be aware of, and trained to exercise their responsibilities towards information security. However in traditional educational models there are usually a percentage of the learners who do not pass the course, or in other words, successfully meet the assessment criteria. In order for an organization’s information to be secure, everyone needs to not only be trained, but to “pass” the training. Unlike traditional education, failing an information security educational program cannot be accepted. Workers at every level, even those who do not use a computer, are liable to be targeted (Mitnick & Simon, 2002, p. 39). This means that having even a single person who does not know his/her information security responsibilities should be unacceptable.

3.2 Employees must know why information security is important and why a specific policy or control is in place.

Recent studies have suggested that current information security awareness programs are failing (Siponen, 2001). This failure is due to many reasons. Schlienger & Teufel (2003) have shown that even employees who know their responsibilities with regards to information security will still disobey security policy if they disagree with the policy. They suggest that the mere awareness of the policies and procedures is in fact not sufficient, the users also need to know why a specific policy or control is in place (Schlienger & Teufel, 2003). In information security, being taught why a specific policy or control is in place is generally considered to be a feature of education, and not of awareness (Schlienger & Teufel, 2003; NIST, 1998, pp. 16-17). Information security “education” is generally sub-divided into three levels, namely; awareness, training and education. Awareness simply focuses attention on information security. Training is more interactive and tries to instill the necessary skills and competencies. Education integrates all of the security skills and competencies of the various functional specialties into a common body of knowledge and adds a multi-disciplinary study of concepts, issues, and principles (NIST, 1998, pp. 15-16). A feature of the educational level is that the user must understand why information security is important (Schlienger & Teufel, 2003; NIST, 1998, pp. 16-17). Obviously end-users do not require the same level of understanding as information security professionals (NIST, 1998, p. 14). You don’t need to understand why procedures are in place or how the technologies work to use them.
effectively (Tripathy, 2000; NIST 1998, p. 15). However, in information security, if a user asks why, it should always be explained (Tripathy, 2000).

3.3 Learning materials should be customized to the needs of individual learners.

In an organizational context, users of information exist at several levels. There are essentially three categories of users that need to be educated in information security awareness namely: The End User, IT Personnel and Top Management (Thompson, 1998). The National Institute for Science and Technology (NIST) expands on this classification by stating that training and education are to be provided selectively, based on individual responsibilities and needs. Specifically, training is to be provided to individuals based on their particular job functions (NIST, 1998, p. 43). The ISO/IEC 17799 states that the information security policy should be communicated throughout the organization to users in a form that is relevant, accessible and understandable to the intended reader (BSI, 1999, p. 3). According to NIST, individuals learn in several ways, but each person, as part of his/her personality, has a preferred or primary learning style. Instruction can positively, or negatively, affect a student’s performance, depending on whether it is matched, or mismatched, with a student’s preferred learning style (NIST, 1998, p. 19). Thus, what should be taught to a specific individual user and how it should be taught, will depend on both the user’s preferred learning style, and the specific role that user plays within the organization.

3.4 Users should be responsible for their own learning.

In today’s organizations it is crucial to maximize return on investment. Through its very nature classroom training requires the availability of highly trained specialists to present the courses. It also requires that the learners take time off from their regular duties to attend classes. These factors make classroom training very expensive. One of the most cost-effective substitutes for traditional classroom training is to provide employees with intranet-based instruction (O’Brien, 1999, p.361). Such web-based instructional programs require individual learners to be responsible for their own acquisition of knowledge instead of being passive receptors in the process (ITiCSE Working Group on the Web and Distance Learning, 1997). Self-driven learning also enables organizations to make learning material available in a variety of formats. This is turn means users will have a choice of how they
are taught, which has already been shown to be a necessary feature of information security education.

3.5 **Users should be held accountable for their studies.**

Most information security standards make it clear that users should be held accountable for their information security **responsibilities** (BSI, 1999, pp. 8-10). These responsibilities are normally spelt out in the organization’s information security policies and procedures. In an organization, policies function in a similar fashion to laws. For laws, ignorance is not a valid defense. However ignorance of policy is an acceptable defense (Whitman & Mattord, 2003, p. 93). Thus, to be able to hold employees accountable for their **actions**, the organization should have proof, normally in the form of a signed form, that the employees have been educated regarding their responsibilities and that they understand and accept these responsibilities as laid out in the policies (Whitman & Mattord, 2003, p. 93). Wood (1997) suggests that all employees should be required, on an annual basis, to sign a statement saying that they have read and understood the information security policy manual. It should thus be clear that self-driven learning for information security purposes, as discussed previously, could only be used if the employees are also held accountable for their learning. Otherwise the organization could not legally hold the employees accountable for their actions.

Many organizations have realized that their own employees are the biggest threat to their information systems (Von Solms, 2000). However, through the establishment of a culture of information security, users can become a security asset instead of being a threat (Von Solms, 2000). Education of employees plays a very important role in the establishment of such a culture. It is paramount that the people are educated to want to be more secure in their day to day operation (Nosworthy, 2000). Such a change of attitude is of utmost importance, because a change in attitude automatically leads to a subsequent behavioral change (Nosworthy, 2000). The employees can then become the organization’s most valuable assets. Current programs used to educate employees, fails to pay sufficient attention to aspects related to the behavioral sciences (Siponen, 2001).

It would make sense to adhere to a formal educational methodology when constructing such educational programs. The methodology used should be suitable for the specific needs of an information security user education program. Since the aim of the user education program is not to prepare the users for further levels of formal education, but rather to help them achieve