河南工業大學

毕业设计(论文)外文资料翻译

中文题目: 信息安全管理是工业界的信息安全检索和意识模型

外文题目 Information security management an information security retrieval and awareness model for industry

院系名称: 信息科学与工程学院 专业班级: 软件工程 1503

学生姓名: 王进 学 号: 201516920522

指导教师: 程凤娟 教师职称: 副教授

起止日期: 2019 年 1 月 11 日-2019 年 3 月 5 日 地 点: 莲花街校区

附 件: 1.外文资料翻译译文; 2.外文原文。

指导教师评语:

指导教师签字: 2019 年 3 月 5 日

附件 1：外文资料翻译译文

信息安全管理是工业界的信息安全检索和意识模型

1.介绍

在当今竞争激烈的商业环境中，信息就是许多组织的生命线。 因此，应相应地对其进行保护和管理（Broderick，2001;Finne，2000;Posthumus 和 Von Solms，2004; Squara，2000）。如果由于任何原因，信息受到损害，组织可能会浪费时间，人力，金钱或商业机会（Dhillon 和 Moores，2001; Whiteman 和 Mattord，2003）。这种信息保护称为“信息安全管理”。信息安全的主要目标是保护信息并确保信息的可用性，机密性和完整性不受任何损害（Aljifri 和 Navarro，2003; Finne，2000; 国家标准研究所，2000; Pfhleeger，1997;Von Solms，1999）。信息安全管理就是要确保通过积极主动的管理来保障信息安全，信息安全风险，威胁和漏洞。

信息安全管理应该建立在日常业务运营中，而不是被视为可选的额外业务（Lewis，2000）。构成信息安全管理一部分的一个重要方面是信息安全意识（Deloitte al，2005; Lewis，2000; Nosworthy，2000; Schultz，2004;Thomson 和 Von Solms，1998; Wood，1995）。 信息安全意识是确保所有员工意识到他们的角色和责任,确保他们使用的信息（Irvine et al，1998;Wright，2004; Thomson 和 Von Solms，1998; Wright，1998）。根据 Deloitte et al（2005 年），约占全球的 45％组织对员工的信息安全威胁问题不敏感，以及缺乏信息安全意识很可能导致组织内的信息泄露。这是管理层确保信息安全意识的政策和程序没有做好。

本文的目的是提出一个概念性的观点。一种信息安全检索和意识模型可以被业界用来增强员工的信息安全意识。第一部分将被投票给一个共同的知识体系用于特别适合工业的信息安全将拟议模型的基础。第二部分将致力于识别典型组织中的不同利益相关者，并根据这些利益相关者进行分组他们的工作类别。最后，本文将最终提出信息安全检索和信息安全检索的概念工业意识（ISRA）模型。

2.适合行业的共同的信息安全知识体系

信息安全知识体系是当来自全球的信息被分组时一起用于作为如何使用的指南保护信息（Fraser，1997）。虽然正在不断努力建立，但没有被普遍接受的信息安全共同知识体系（Crowley，2003 年）。在这样一个知识体系的发展中出现的限

制是，它经常主要针对工业界的专业人士，并且没有留下任何空间或低级别用户（如最终用户）的机会，他们需要这种知识的缩小版本（CSI / FBI，2005;Wilson and Hash，2005）。共同点是信息安全检索和意识模型的基础的一部分，开发的知识在本文中有两个方面：专注于保护那些在信息安全方面没有正式背景或没有背景的用户，同时也不排除专业人士。

目前适用于工业的信息安全的共同知识体系正在发展：通常非道德和法律问题等非技术性，与人类相关的问题不会得到与技术问题（如加密）一样受到关注（Deloitte et al，2005; Posthumus和Von Solms，2004; Sipo-nen，2000; Von Solms，2001; Wright，1998）。应该平衡信息安全的非技术性问题，以确保技术问题不会掩盖非技术性问题，在制定共同点时，充分解决了信息安全的人性问题使适合工业的信息安全知识体系。这样的知识体系应该以领导国家为基础和国际信息安全为主，以确保所有信息安全问题（技术以及非技术性问题得到解决）。

信息安全的共同知识体系针对本文提出的工业指标，旨在解决当前这些知识体系发展中的这些局限性（见图1）。各种最先进的国家和国际知识信息安全文件被用作基础拟议的信息安全知识体系。这些文件由顶级信息汇编安全专业人员处理有关信息安全的实施和管理的问题。由于纸张长度，这些文件的内容没有进一步讨论，读者应该咨询参考文献更多细节（COBIT，2001; GMITS，2001; ISO /IEC177799,2000; IT Governance Institute，2001a，b;国家标准技术研究所，2000）。

拟议的共同知识体系分为技术信息安全问题和非技术信息安全问题 - 如图1所示。首先，这种划分将确保那些信息安全问题相关的低级用户可以更容易识别，因为这些问题将主要落入非技术性的建议的共同知识体系的一面。其次，这个部门将确保技术信息安全问题不会掩盖非技术信息安全问题。请注意，描述的信息安全问题列表在图1中并非详尽无遗，而仅仅是一些例子涉及的信息安全问题。

技术信息安全问题主要集中在安全和保护信息所需的技术导向的知识和工具（如加密技术）（Smith et al，2004）。这些具有适当的安全知识和工作经验的技术部门和员工大多受到限制。其知识通常通过正式资格获得，如高等学位/文凭或与行业相关的信息安全课程。非技术信息安全问题，它包括道德，法律问题等。这个非技术部分也可以考虑保护信息系统和保护信息管理方面。

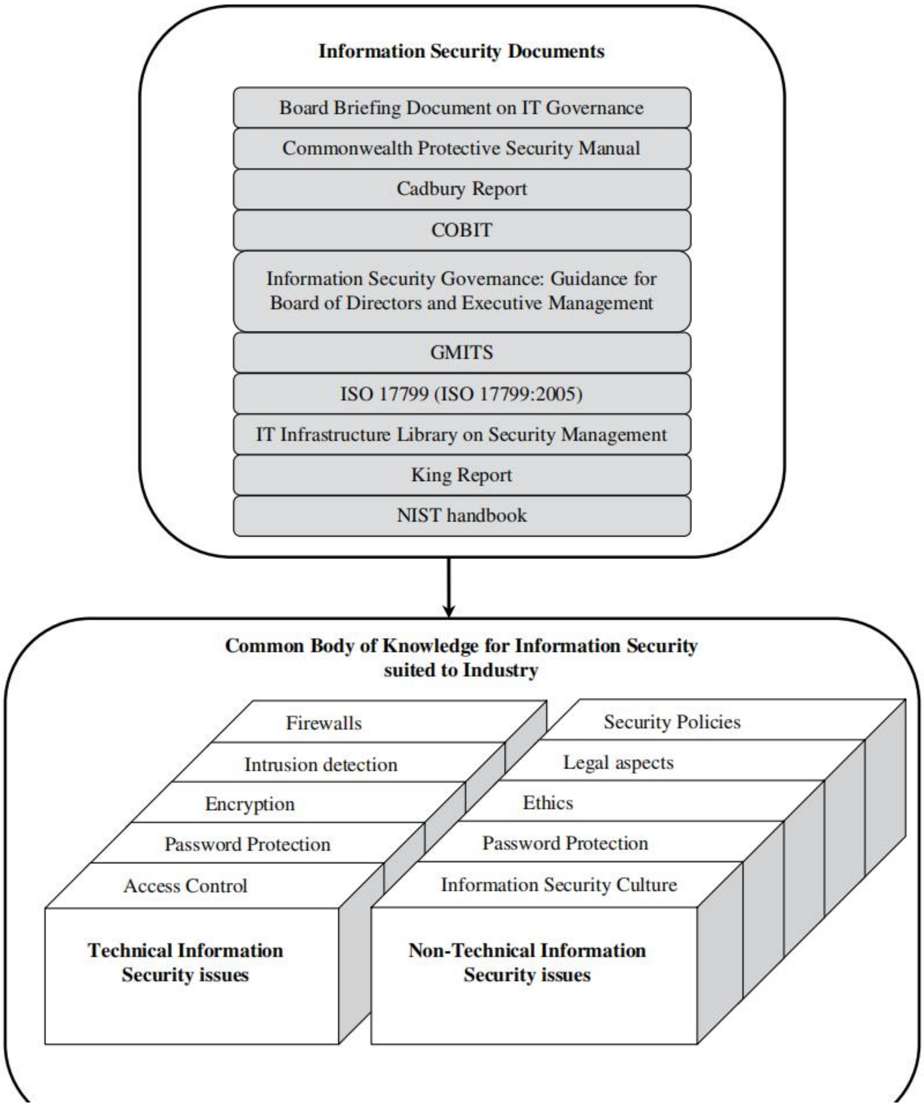

Information Security Documents
Board Briefing Document on IT Governance
Commonwealth Protective Security Manual
Cadbury Report
COBIT
Information Security Governance: Guidance for Board of Directors and Executive Management
GMITS
ISO 17799 (ISO 17799:2005)
IT Infrastructure Library on Security Management
King Report
NIST handbook
Common Body of Knowledge for Information Security suited to Industry
Firewalls
Intrusion detection
Encryption
Password Protection
Access Control
Technical Information Security issues
Security Policies
Legal aspects
Ethics
Password Protection
Information Security Culture
Non-Technical Information Security issues

图 1 - 适用于工业的信息安全的共同知识体系

其重点领域涉及不同人类可以对信息和信息系统产生影响。这些人类影响可分为有意或无意，以及它们可能来自组织外部或组织内部。一些信息安全问题可能是两者的一部分或技术和非技术组成部分，例如密码保护（见图 1）。技术人员在网络上安装软件来管理软件时，密码保护可被视为技术问题使用密码。另一方面，密码保护可以在某种情况下被视为非技术性问题，由用户选择安全密码。

在大多数情况，信息安全问题将成为技术或非技术组成部分的一部分适合工业信息安全知识体系。本文提出的信息安全检索和意识模型将专注于非技术信息安全问题。主要原因是关于这个问题已经做了很多研究。然而，对非技术信息安全的研究起因是最近人类有关信息安全问题讨论，非技术信息安全问题一直被忽视（CSI / FBI，2005; Deloitte，2005; Von Solms，2001）。

最先进的国家和国际信息安全文件和非技术信息安全问题拟议的信息安全体系适合本文提出的信息安全检索和意识模型。

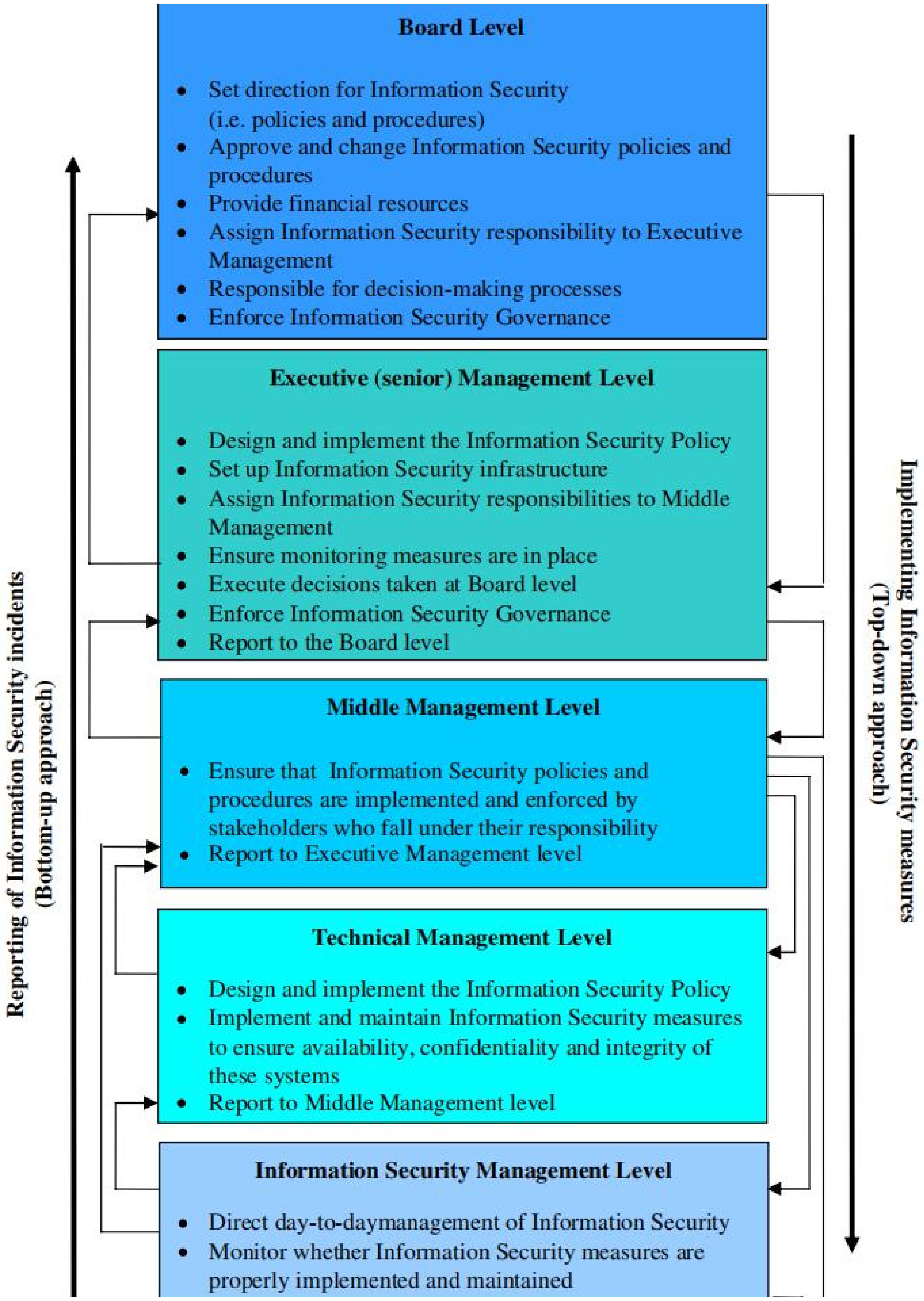
3.IT 权限级别

信息安全检索的第三个模块和意识模型是 IT 权限级别。一个 IT 权威级别由一组利益相关者组成（国家标准与技术研究所，2000 年）。该利益相关者根据工作类别分组在一起，例如高管（国家标准技术研究所，2000）。可以为每个组分配信息安全角色和职责。这将确保这一点特定的 IT 权限级别不会包含大量无关的信息安全文档而过载。相反，它只会保障收到的基本信息是 IT 权限级别使用的特定信息。根据工作条件创建 IT 权限级别时，应该记住组织中的工作类别因组织而异。因此，不同组织的 IT 权限级别也会有所不同（Kisin，1996; National Institute of Standards and Technology，2000; Siponen，2001;Thomson，1999 年;Whiteman and mattord，2003）。为了本文的目的，组织中的利益相关者分为六个 IT 权限级别，如图 2 所示。图 2 提供了有关这些 IT 权限级别的信息安全性的主要责任的总和。

第一个 IT 权限级别是所谓的董事会级别，被广泛认为是最高的 IT 权威级别一个典型的组织（Kisin，1996; National Institute of Standards and Technology，2000; Siponen，2001;Thomson，1999; Whiteman 和 Mattord，2003）。

董事会最终通过适当的信息安全管理确保管理层，组织中的信息不以任何方式泄露。只有董事会发挥积极作用在信息安全和信息安全管理方面，其他 IT 权威级别也会如此（国家标准技术研究所，2000; White -man and Mattord，2003）。

第二个IT权限级别是执行管理这个级别通常包括首席执行官，他可以直接向董事会提供数据。如果是执行管理层与董事会层面密切合作，其中许多是责任将重叠，例如确保适当的信息安全治理（即，通过该系统或方法）公司指导，控制和管理组织（Andersen，2001; IT Governance Institute，2001）。因此，执行管理层应确保执行董事会层面的决策正常。中层管理构成第三个IT权威级别并且通常由不同的部门负责人或部门组成。这个级别应该确保所有信息安全政策和程序正确实施由他们所有依赖其利益相关者执行（Nosworthy，2000）。



Board Level

- Set direction for Information Security (i.e. policies and procedures)
- Approve and change Information Security policies and procedures
- Provide financial resources
- Assign Information Security responsibility to Executive Management
- Responsible for decision-making processes
- Enforce Information Security Governance

Executive (senior) Management Level

- Design and implement the Information Security Policy
- Set up Information Security infrastructure
- Assign Information Security responsibilities to Middle Management
- Ensure monitoring measures are in place
- Execute decisions taken at Board level
- Enforce Information Security Governance
- Report to the Board level

Middle Management Level

- Ensure that Information Security policies and procedures are implemented and enforced by stakeholders who fall under their responsibility
- Report to Executive Management level

Technical Management Level

- Design and implement the Information Security Policy
- Implement and maintain Information Security measures to ensure availability, confidentiality and integrity of these systems
- Report to Middle Management level

Information Security Management Level

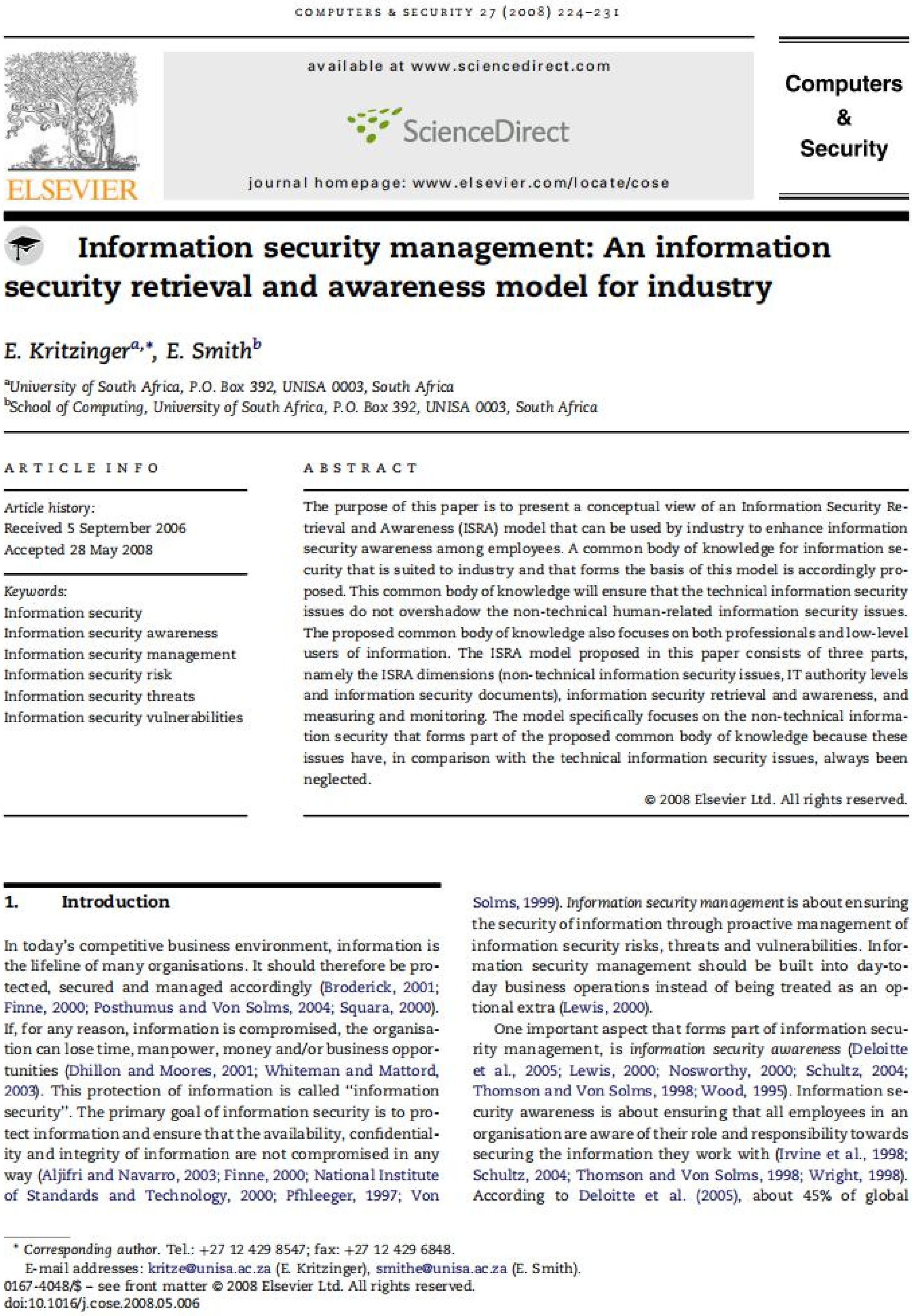
- Direct day-to-daymanagement of Information Security
- Monitor whether Information Security measures are properly implemented and maintained

Reporting of Information Security incidents
(Bottom-up approach)
Implementing Information Security measures
(Top-down approach)

图 2 – IT 权限级别

附件 2：外文原文

节选：



COMPUTERS & SECURITY 27 (2008) 224–231

available at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

ELSEVIER

Computers & Security

Information security management: An information security retrieval and awareness model for industry

E. Kritzinger[a,*], E. Smith[b]

[a]University of South Africa, P.O. Box 392, UNISA 0003, South Africa
[b]School of Computing, University of South Africa, P.O. Box 392, UNISA 0003, South Africa

ARTICLE INFO

Article history:
Received 5 September 2006
Accepted 28 May 2008

Keywords:
Information security
Information security awareness
Information security management
Information security risk
Information security threats
Information security vulnerabilities

ABSTRACT

The purpose of this paper is to present a conceptual view of an Information Security Retrieval and Awareness (ISRA) model that can be used by industry to enhance information security awareness among employees. A common body of knowledge for information security that is suited to industry and that forms the basis of this model is accordingly proposed. This common body of knowledge will ensure that the technical information security issues do not overshadow the non-technical human-related information security issues. The proposed common body of knowledge also focuses on both professionals and low-level users of information. The ISRA model proposed in this paper consists of three parts, namely the ISRA dimensions (non-technical information security issues, IT authority levels and information security documents), information security retrieval and awareness, and measuring and monitoring. The model specifically focuses on the non-technical information security that forms part of the proposed common body of knowledge because these issues have, in comparison with the technical information security issues, always been neglected.

1. Introduction

In today's competitive business environment, information is the lifeline of many organisations. It should therefore be protected, secured and managed accordingly (Broderick, 2001; Finne, 2000; Posthumus and Von Solms, 2004; Squara, 2000). If, for any reason, information is compromised, the organisation can lose time, manpower, money and/or business opportunities (Dhillon and Moores, 2001; Whiteman and Mattord, 2003). This protection of information is called "information security". The primary goal of information security is to protect information and ensure that the availability, confidentiality and integrity of information are not compromised in any way (Aljifri and Navarro, 2003; Finne, 2000; National Institute of Standards and Technology, 2000; Pfhleeger, 1997; Von Solms, 1999). *Information security management* is about ensuring the security of information through proactive management of information security risks, threats and vulnerabilities. Information security management should be built into day-to-day business operations instead of being treated as an optional extra (Lewis, 2000).

One important aspect that forms part of information security management, is *information security awareness* (Deloitte et al., 2005; Lewis, 2000; Nosworthy, 2000; Schultz, 2004; Thomson and Von Solms, 1998; Wood, 1995). Information security awareness is about ensuring that all employees in an organisation are aware of their role and responsibility towards securing the information they work with (Irvine et al., 1998; Schultz, 2004; Thomson and Von Solms, 1998; Wright, 1998). According to Deloitte et al. (2005), about 45% of global

[*] *Corresponding author.* Tel.: +27 12 429 8547; fax: +27 12 429 6848.
E-mail addresses: kritze@unisa.ac.za (E. Kritzinger), smithe@unisa.ac.za (E. Smith).

0167-4048/$ – see front matter © 2008 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2008.05.006

organisations do not sensitise their employees in respect of possible information security threats, and this lack of information security awareness could well lead to compromised information within the organisation. It is the responsibility of management to ensure that information security awareness policies and procedures are in place.

The purpose of this paper is to present a conceptual view of an Information Security Retrieval and Awareness model that can be used by industry in order to enhance the information security awareness of employees. The first part will be devoted to the presentation of a common body of knowledge for information security specifically suited to industry, which will be used as a basis for the proposed model. The second part will be devoted to identifying different stakeholders in a typical organisation and grouping these stakeholders according to their job category. Finally, the paper will culminate in proposing the concept of an Information Security Retrieval and Awareness (ISRA) model for industry.

2. Common body of knowledge for information security suited to industry

A common body of knowledge for information security is formed when information from around the globe is grouped together for the purpose of being used as a guideline on how to secure information (Fraser et al., 1997). There are, however no universally accepted common body of knowledge for information security, though ongoing efforts are made to establish one (Crowley, 2003). A limitation that occurs in current developments of such a body of knowledge, is that it frequently focuses primarily on *professionals* in industry and leaves no room or opportunity *for low-level users* (such as end users) who require a scaled-down version of this knowledge (CSI/FBI, 2005; Wilson and Hash, 2005). The aim of the common body of knowledge that is developed as part of the basis for the Information Security Retrieval and Awareness model proposed in this paper is twofold: to focus specifically on users with little or no formal background on how to properly secure information they work with, yet also not to exclude professionals.

There is a further limitation in current developments regarding a common body of knowledge for information security suited to industry: very often the non-technical, human-related issues such as ethics and legal issues do not receive as much attention as the technical issues (such as encryption) (Deloitte et al., 2005; Posthumus and Von Solms, 2004; Siponen, 2000; Von Solms, 2001; Wright, 1998). The technical and non-technical issues of information security should be balanced to ensure that the *technical issues do not overshadow the non-technical issues* and that the human side of information security is adequately addressed when developing a common body of knowledge for information security suited to industry. Such a body of knowledge should be based on leading national and international information security documents to ensure that all information security issues (technical as well as non-technical) are addressed.

The common body of knowledge for information security tailored towards industry that is proposed in this paper therefore aims to address both these limitations in current developments of such common bodies of knowledge (see Fig. 1).

Various state-of-the-art national and international accepted Information Security documents are used as basis for the proposed common body of knowledge for Information Security. These documents were compiled by top Information Security professionals and contain information regarding the implementation and management of Information Security issues. Due to paper length, the content of these documents are not discussed further and the reader should consult the references for more detail (COBIT, 2001; GMITS, 2001; ISO/IEC177799, 2000; IT Governance Institute, 2001a,b; National Institute of Standards and Technology, 2000).

The proposed common body of knowledge is divided into technical information security issues and non-technical information security issues – as depicted in Fig. 1. Firstly, this division will ensure that those information security issues relevant to *low-level users* can be identified more easily, because such issues will fall primarily into the non-technical side of the proposed common body of knowledge. Secondly, this division will ensure that *the technical information security issues do not overshadow the non-technical information security issues*. Note that the list of information security issues depicted in Fig. 1 is not exhaustive, but merely an example of some of the information security issues involved.

The technical information security issues focus mainly on the technical-oriented knowledge and tools (such as encryption techniques) that are required to secure and protect information (Smith et al., 2004). These issues are mostly confined to the technical departments and employees with proper information security knowledge and work experience. Their knowledge is usually obtained through formal qualifications, such as tertiary degrees/diplomas or industry-related information security courses.

The non-technical information security issues include all the non-technical-oriented knowledge that is required to secure and protect information and information systems. It includes issues such as ethics, legal issues and information security culture. This non-technical part can also be considered the management side of securing and protecting information and information systems. Its focal area involves the different effects that humans can have on the security and protection of information and information systems. These human influences can be classified as intentional or accidental, and they may originate from either outside or within an organisation.

Some information security issues may be part of both the technical and the non-technical components of the common body of knowledge for information security suited to industry, for example password protection (see Fig. 1). Password protection can be viewed as a *technical* issue in instances where technical personnel install software on the network to regulate the use of passwords. On the other hand, password protection can be considered as a non-technical issue in a situation where it is up to the user to choose a secure password. In the majority of cases however, information security issues will be part of *either* the technical *or* the non-technical components of the common body of knowledge for information security suited to industry.

The Information Security Retrieval and Awareness model proposed in this paper will focus exclusively on the *non-technical* information security issues. The primary reason for this is that much research has already been done regarding the implementation of technical information security issues in

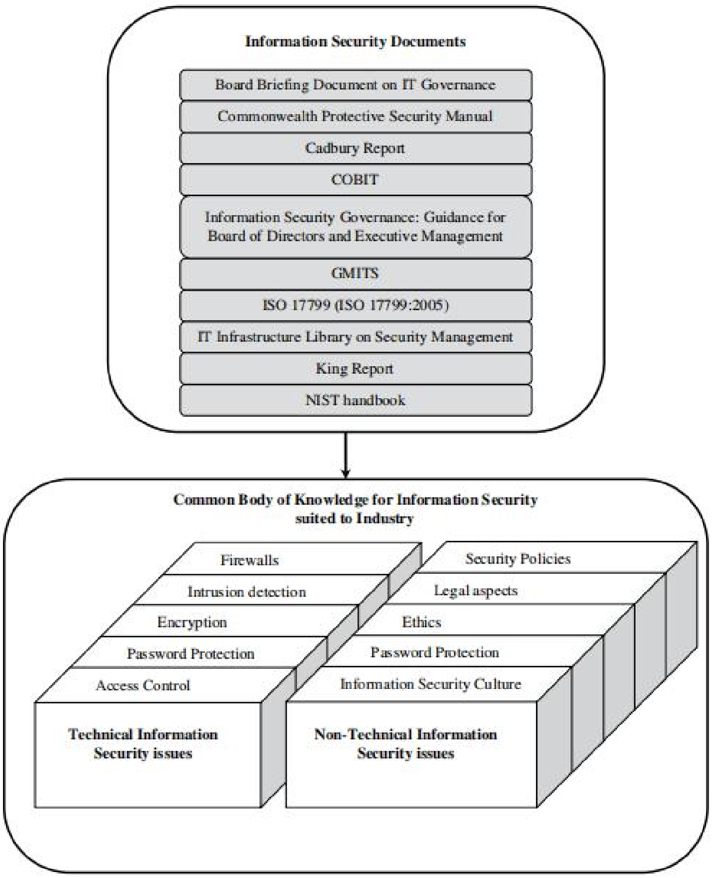

Information Security Documents
Board Briefing Document on IT Governance
Commonwealth Protective Security Manual
Cadbury Report
COBIT
Information Security Governance: Guidance for Board of Directors and Executive Management
GMITS
ISO 17799 (ISO 17799:2005)
IT Infrastructure Library on Security Management
King Report
NIST handbook
Common Body of Knowledge for Information Security suited to Industry
Firewalls
Intrusion detection
Encryption
Password Protection
Access Control
Technical Information Security issues
Security Policies
Legal aspects
Ethics
Password Protection
Information Security Culture
Non-Technical Information Security issues

Fig. 1 – Common body of knowledge for information security suited to Industry.

industry. Research into non-technical information security issues, however, emerged only recently and the human-related information security issues have – in comparison with the technical information security issues – been neglected so far (CSI/FBI, 2005; Deloitte et al., 2005; Von Solms, 2001).

The state-of-the-art *national and international information security documents* and the *non-technical information security issues* of the proposed common body of knowledge for information security suited to industry constitute the first two building blocks of the Information Security Retrieval and Awareness model proposed in this paper.

3. IT authority levels

The third building block of the Information Security Retrieval and Awareness model is the IT authority levels. An IT authority level consists of a group of stakeholders who are the people who ensure the survival of the organisation (National Institute of Standards and Technology, 2000). The stakeholders are grouped together according to job category, for example executives (National Institute of Standards and Technology, 2000). Information security roles and responsibilities could be assigned to each group. This would ensure that a specific IT authority level is not overburdened with an enormous amount of information security documents that might include a large amount of irrelevant information. Instead, it would receive only the essential information needed to secure the specific information the IT authority level works with.

When creating IT authority levels according to job category, one should remember that job categories in organisations will differ from organisation to organisation and therefore the IT authority levels will also be different in different organisations (Kisin, 1996; National Institute of Standards and Technology, 2000; Siponen, 2001; Thomson, 1999; Whiteman and Mattord, 2003). For the purpose of this paper, the stakeholders in a typical organisation are grouped into six IT authority levels, as depicted in Fig. 2. Fig. 2 provides a summary of the primary responsibilities regarding information security for each of these IT authority levels.

The first IT authority level is the so-called Board level, which is widely recognised as the highest IT authority level of a typical organisation (Kisin, 1996; National Institute of Standards and Technology, 2000; Siponen, 2001; Thomson, 1999; Whiteman and Mattord, 2003). The Board is ultimately responsible for ensuring, through proper information security management, that information in the organisation is not compromised in any way. Only if the Board plays a proactive role in information security and information security management will the rest of the IT authority levels follow suit (National Institute of Standards and Technology, 2000; Whiteman and Mattord, 2003).

The second IT authority level is the Executive Management level and this will typically include the CEO, who is directly accountable to the Board. If the Executive Management level works very closely with the Board level, many of their

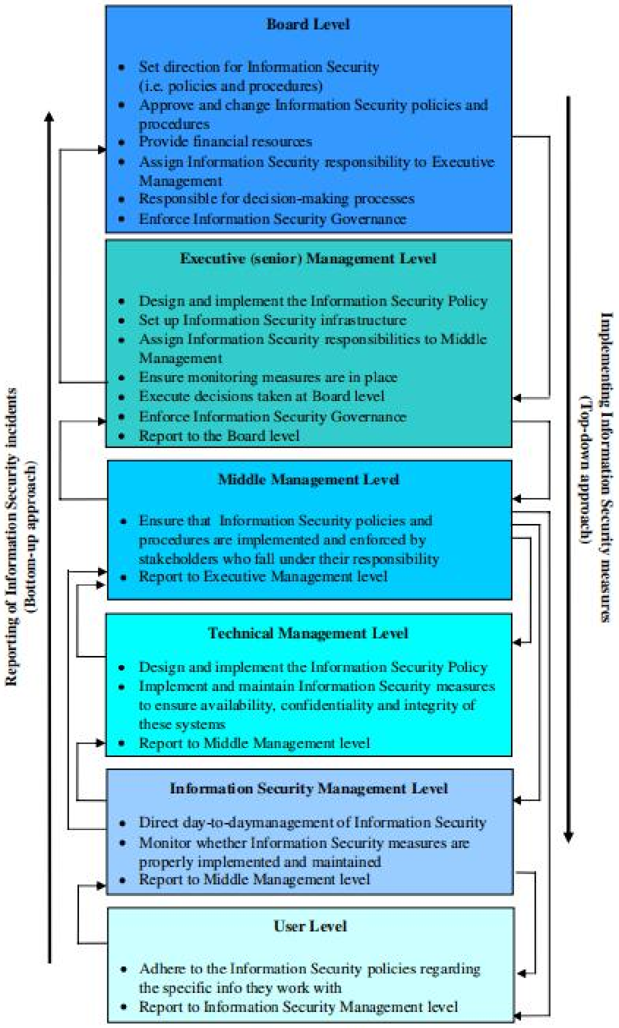

Board Level
• Set direction for Information Security (i.e. policies and procedures)
• Approve and change Information Security policies and procedures
• Provide financial resources
• Assign Information Security responsibility to Executive Management
• Responsible for decision-making processes
• Enforce Information Security Governance
Executive (senior) Management Level
• Design and implement the Information Security Policy
• Set up Information Security infrastructure
• Assign Information Security responsibilities to Middle Management
• Ensure monitoring measures are in place
• Execute decisions taken at Board level
• Enforce Information Security Governance
• Report to the Board level
Middle Management Level
• Ensure that Information Security policies and procedures are implemented and enforced by stakeholders who fall under their responsibility
• Report to Executive Management level
Technical Management Level
• Design and implement the Information Security Policy
• Implement and maintain Information Security measures to ensure availability, confidentiality and integrity of these systems
• Report to Middle Management level
Information Security Management Level
• Direct day-to-daymanagement of Information Security
• Monitor whether Information Security measures are properly implemented and maintained
• Report to Middle Management level
User Level
• Adhere to the Information Security policies regarding the specific info they work with
• Report to Information Security Management level
Reporting of Information Security incidents
(Bottom-up approach)
Implementing Information Security measures
(Top-down approach)

Fig. 2 – IT authority levels.