



ELSEVIER

Available online at [www.sciencedirect.com](http://www.sciencedirect.com)

ScienceDirect

journal homepage: [www.elsevier.com/locate/cose](http://www.elsevier.com/locate/cose)Computers  
&  
Security

## Information security conscious care behaviour formation in organizations



CrossMark

Nader Sohrabi Safa<sup>a,\*</sup>, Mehdi Sookhak<sup>a,1</sup>, Rossouw Von Solms<sup>b,2</sup>,  
Steven Furnell<sup>c,3</sup>, Norjihani Abdul Ghani<sup>a,4</sup>, Tutut Herawan<sup>a,5</sup>

<sup>a</sup> Department of Information Science, Faculty of Computer Science & Information Technology, University of Malaya, 50603 Kuala Lumpur, Malaysia

<sup>b</sup> Centre for Research in Information and Cyber Security, Nelson Mandela Metropolitan University, Port Elizabeth, South Africa

<sup>c</sup> Centre for Security, Communications and Network Research, Plymouth University, United Kingdom

### ARTICLE INFO

#### Article history:

Received 29 November 2014

Received in revised form

25 April 2015

Accepted 25 May 2015

Available online 3 June 2015

#### Keywords:

Information security

Conscious care behaviour

Awareness

Risk

Organization policy

### ABSTRACT

Today, the Internet can be considered to be a basic commodity, similar to electricity, without which many businesses simply cannot operate. However, information security for both private and business aspects is important. Experts believe that technology cannot solely guarantee a secure environment for information. Users' behaviour should be considered as an important factor in this domain. The Internet is a huge network with great potential for information security breaches. Hackers use different methods to change confidentiality, integrity, and the availability of information in line with their benefits, while users intentionally or through negligence are a great threat for information security. Sharing their account information, downloading any software from the Internet, writing passwords on sticky paper, and using social security numbers as a username or password are examples of their mistakes. Users' negligence, ignorance, lack of awareness, mischievous, apathy and resistance are usually the reasons for security breaches. Users' poor information security behaviour is the main problem in this domain and the presented model endeavours to reduce the risk of users' behaviour in this realm. The results of structural equation modelling (SEM) showed that Information Security Awareness, Information Security Organization Policy, Information Security Experience and Involvement, Attitude towards information security, Subjective Norms, Threat Appraisal, and Information Security Self-efficacy have a positive effect on users' behaviour. However, Perceived Behavioural Control does not affect their behaviour significantly. The Protection Motivation Theory and Theory of Planned Behaviour were applied as the backbone of the research model.

© 2015 Elsevier Ltd. All rights reserved.

\* Corresponding author. Tel.: +60 102402372.

E-mail addresses: [sohrabisafa@yahoo.com](mailto:sohrabisafa@yahoo.com) (N.S. Safa), [m.sookhak@ieee.org](mailto:m.sookhak@ieee.org) (M. Sookhak), [Rossouw.VonSolms@nmmu.ac.za](mailto:Rossouw.VonSolms@nmmu.ac.za) (R. Von Solms), [S.Furnell@plymouth.ac.uk](mailto:S.Furnell@plymouth.ac.uk) (S. Furnell), [norjihani@um.edu.my](mailto:norjihani@um.edu.my) (N.A. Ghani), [tutut@um.edu.my](mailto:tutut@um.edu.my) (T. Herawan).

<sup>1</sup> Tel.: +60 177614849.

<sup>2</sup> Tel.: +27 415049604.

<sup>3</sup> Tel.: +44 1752586234.

<sup>4</sup> Tel.: +60 125432935.

<sup>5</sup> Tel.: +60 142723760.

<http://dx.doi.org/10.1016/j.cose.2015.05.012>

0167-4048/© 2015 Elsevier Ltd. All rights reserved.

---

## 1. Introduction

Advances in web-based oriented technologies and services are taking place with significant speed around the world. However, information security is still a prevalent issue among experts as well as users. Companies and their e-Customers are concerned about cyber-attacks, and, consequently, are keen to minimize information security risk (Safa and Ismail, 2013). The Internet is a vast network and has great potential for threats. Online attackers use new and different methods for achieving security breaches. Recently, hackers have developed a fake website and asked users to download free anti-virus software from their website. Many users downloaded the antivirus software from these fake websites and lost their private information (Kim et al., 2015). Technology and the threat environment change frequently, and are dynamic due to their nature. For instance, the Internet of Things (IoT) shows the vast number of new applications on the Internet that connects devices, systems, services and even smart objects, and covers a variety of protocols, domains, and applications. These changes make it difficult to anticipate and quantify the information security risk (Pfleeger and Caputo, 2012). Conscious care behaviour is an effective approach to counter creative attacks. Conscious care behaviour means that users think about the consequences of their actions in terms of information security when they work with a system, particularly on the Internet. Information security awareness, knowledge and experience play vital roles in this domain. Rhee et al. (2009) asserted that information security risk management encompasses two aspects: 1) security software and features, such as pop-up blocking function, anti-spyware, and anti-virus software; 2) security conscious care behaviour related to computer and Internet usage.

Experts believe that the technology aspects of information security cannot solely guarantee a secure environment and that human information security behaviour should be taken into consideration (Furnell and Clarke, 2012). The importance of human factors in the domain of information security cannot be understated. Information security management should consider users and their perceptions as important factors to provide a secure environment. In other words, users are the centre of the security concept. Mitigating and preventing cyber security risks need to be implemented in several stages, and behavioural science plays an important role in the stages of the design, development and maintenance of web systems (Padayachee, 2012). Users consider security as an obstacle when there is no appropriate response to their cyber incidents. They may be faced with difficulties in security implementation, and misinterpret, mistrust or override the security (Cox, 2012). Users' attitudes and their resistance behaviour change when they face a mandatory password change. Researchers have realized that such changes are intentionally delayed and are considered an unnecessary interruption. They know that a password breach can have severe consequences, but do not change their attitude towards the implementation of a security policy (Stanton et al., 2005). Users, intentionally or through negligence, are an important threat to information security, in which careless information security behaviour is the main problem. This

research aims to change users' behaviour to conscious care behaviour in the domain of information security.

The remainder of this paper is organised as follows. Section two presents two fundamental theories, the Theory of Planned Behaviour (TPB) and the Protection Motivation Theory (PMT), as the background of this research. Different parts of the model and hypotheses are then discussed in section three. The research methodology describes the stages of problem solving and is presented in section four. Data analysis and the results of the measurement model and structural model are discussed in section five. The contribution and implementation of the research are presented in section six, and, finally, overall conclusions and thoughts towards future work can be found in section seven.

---

## 2. Theoretical background

Human behaviour can change based on one's attitude, which is a salient point that we applied to change information security behaviour to conscious care behaviour. Behaviour is driven by behavioural intention where the behavioural intention is a function of an individual's attitude towards the behaviour (Ajzen and Madden, 1986). The Theory of Planned Behaviour (TPB) and Protection Motivation Theory (PMT) are the backbone of the research model and explain how the users' behaviour can change to conscious care behaviour.

### 2.1. Theory of planned behaviour

Ajzen (1991) proposed the Theory of Planned Behaviour (TPB) to explain the influence of attitude, subjective norms, and perceived behavioural control upon individual behaviour. The TPB has been widely applied in diverse studies to predict individuals' behaviour. Attitude refers to the users' positive or negative feeling towards a particular behaviour, and is defined as a learned tendency to evaluate things in a particular way. The evaluation can be positive or negative about an object, issue, people or events (Leonard et al., 2004). Once the evaluation changes, attitude, and, consequently, behaviour change. Attitude can also be implicit or explicit. In explicit attitude, we are consciously aware, which influences our beliefs and behaviour. In contrast, implicit attitude unconsciously affects our behaviour and beliefs (Albrechtsen and Hovden, 2010). Human knowledge has a direct effect on one's attitude. This effect comes from our direct personal experience or the result of our observations. Different training methods also change our attitude towards certain issues (Abawajy, 2014). Information security awareness of risks influences the attitude towards behaviour in the users (Bryce and Fraser, 2014; Dinev and Hu, 2007). Ifinedo (2014) showed that attitude, subjective norms, and perceived behavioural control influence users' intention to comply with information security organization policies.

In this research, the presented model shows that information security awareness influences the attitude towards having a careful manner in terms of information security behaviour. Subjective norms lead to social pressure on individuals to perform or not perform a behaviour and refer to the users' perception of what people important to them think.

Download English Version:

<https://daneshyari.com/en/article/455840>

Download Persian Version:

<https://daneshyari.com/article/455840>

[Daneshyari.com](https://daneshyari.com)