



Chapter II

A Forensic Computing Perspective on the Need for Improved User Education for Information Systems Security Management

Vlasti Broucek

University of Tasmania, Australia

Paul Turner

University of Tasmania, Australia

ABSTRACT

This chapter is divided to two parts. Part one identifies common security and privacy weaknesses that exist in e-mail and WWW browsers and highlights some of the major implications for organisational security that result from employees' online behaviours. This section aims to raise awareness of these weaknesses amongst users and to encourage administrators to mitigate their consequences through enhanced security and privacy-focused user education and training. Part two makes recommendations for improved user education as a component of information systems security management practices. These recommendations have been generated from a forensic computing perspective

that aims to balance the complex set of issues involved in developing effective IS security management policies and practices. From this perspective these policies and practices should improve security of organisation and the privacy of employees without compromising the potential need for future forensic investigation of inappropriate, criminal, or other illegal online behaviours.

INTRODUCTION

In the age of hacktivism, malware and cyber-warfare, increasing numbers of publications are being produced by computer security specialists and systems administrators on technical issues arising from illegal or inappropriate on-line behaviours. Technical advances — in the ability of information systems to detect intrusions, denial of services attacks and also to enhance network monitoring and maintenance — are well documented and subject to constant research and development.

To date, however, there has been limited research into a range of other issues impacting on information systems (IS) security and its management. From a forensic computing (FC) perspective IS security management emerges as part of a much broader debate on the risks and challenges posed by digitalisation for legal, technical and social structures (Broucek & Turner, 2001a, 2001b). This perspective highlights that IS security management cannot be addressed by technical means alone. Indeed the development of effective security management relies on recognition of the need to balance a complex set of technical, legal and organisational issues (Lichtenstein & Swatman, 2000).

This chapter explores one of these issues, “user education” and identifies its relevance for, and interrelationships with, other IS security management issues. This exploration is conducted through an examination of the two most common Internet applications used in organisations: electronic mail (e-mail) and World Wide Web (WWW) browsers. By identifying common security weaknesses in both types of applications, the chapter examines how the security management problems are compounded by common online user behaviours. Retaining a FC perspective, the chapter makes recommendations for improving IS security management.

PART ONE

At a technical level, systems administrators are very aware of the security risks and security weaknesses prevalent in Internet applications and, in particular, in e-mail and WWW browsers. Significantly, while technical solutions are available (at a cost) to alleviate most of the major security challenges, the manner in which most users continue to utilise these applications compounds organisational IS security problems. While technical responses may be able to treat some of the symptoms of inappro-

6 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/forensic-computing-perspective-need-improved/7383

Related Content

A Secure and Trustful E-Ordering Architecture (TOES) for Small and Medium Size Enterprises (SEMs)

Spyridon Papastergiou and Despina Polemi (2008). *International Journal of Information Security and Privacy* (pp. 14-30).

www.irma-international.org/article/secure-trustful-ordering-architecture-toes/2479

Key Vulnerabilities in Internet of Things: A Holistic View

Kavitha Ammayappan, Arun Babu Puthuparambil and Atul Negi (2020). *Applied Approach to Privacy and Security for the Internet of Things* (pp. 38-54).

www.irma-international.org/chapter/key-vulnerabilities-in-internet-of-things/257903

Globalization and Data Privacy: An Exploratory Study

Robert L. Totterdale (2010). *International Journal of Information Security and Privacy* (pp. 19-35).

www.irma-international.org/article/globalization-data-privacy/46101

Digital Transformation of E-Commerce Services and Cybersecurity for Modernizing the Banking Sector of Pakistan: A Study of Customer Preferences and Perceived Risks

Tansif Ur Rehman (2021). *Handbook of Research on Advancing Cybersecurity for Digital Transformation* (pp. 373-403).

www.irma-international.org/chapter/digital-transformation-of-e-commerce-services-and-cybersecurity-for-modernizing-the-banking-sector-of-pakistan/284160

A Secure Hybrid Network Solution to Enhance the Resilience of the UK Government National Critical Infrastructure TETRA Deployment

Devon Bennett, Hamid Jahankhani, Mohammad Dastbaz and Hossein Jahankhani (2011). *International Journal of Information Security and Privacy* (pp. 1-13).

www.irma-international.org/article/secure-hybrid-network-solution-enhance/53012