Computers & Security (2005) **24**, 448–459

ELSEVIER

Computers & Security

www.elsevier.com/locate/cose

Information security policy's impact on reporting security incidents

Terry L. Wiant

Marshall University, 1 John Marshall Drive, Huntington, WV 25755, USA

Received 20 May 2004; revised 14 October 2004; accepted 28 March 2005

KEYWORDS
Computer abuse;
Deterrence;
Medical records;
Policy;
Incidents;
Seriousness;
Security

Abstract The New Health Privacy Rule, effective from April 14, 2003, has made it illegal for healthcare providers and insurers to release a patient's medical records without the individual's consent [Cropper, Carol Marie. How to keep prying eyes off your medical records. Business Week November 19, 2001;130–2]. Rule provisions dictate that healthcare providers and insurers must have a written information security policy and present it to patients [Cropper, Carol Marie. How to keep prying eyes off your medical records. Business Week November 19, 2001;130–2].

This paper evaluated the utility of having such a policy by examining the reporting of computer abuse incidents and the reporting of the seriousness of computer abuse incidents in those hospitals that either have or do not have a written information security policy. The premise of this study is that for an information security policy to be effective, computer abuse incidents and the seriousness of those computer abuse incidents must be reported.

For this study, there were two factors that were examined for all respondent hospitals. The first factor was the reporting of computer abuse incidents that occurred the year prior to the study. The second factor was the reporting of the seriousness of computer abuse incidents that occurred the year prior to the study.

Survey instruments were distributed to hospitals of various sizes, specialties, ownership, and types. The questionnaire collected information about the reporting of computer abuse incidents and their seriousness level to determine if an information security policy is effective in influencing the reporting of each. In addition, background information was collected from each hospital to aid in the analysis of the survey results.

Introduction

Modern computer applications in the healthcare industry threaten individual information security despite offering significant benefits to patients and practitioners. In any industry, compared to paper based records, computer databases of personally identifiable information may be accessed, changed, viewed, copied, used, disclosed, or deleted more

0167-4048/$ - see front matter © 2005 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2005.03.008

easily and by more individuals, regardless of their official access restrictions. Private or commercial parties can assemble medical profiles by using only a minimum amount of personal data (Chandrasekaran, 1998; O'Harrow, 1998). Such violations in any industry cannot be stopped unless the incidents and their seriousness are reported. Yet only 60% of respondents to the KPMG 2002 Global Information Security Survey have any form of security violation reporting (Global information security survey, 2002). In addition, according to the CSI/FBI 2004 Computer Crime and Security Survey the percentage of organizations reporting computer intrusions to law enforcement has declined over the past year. The primary reason for this decline is the concern over negative publicity (Gordon et al., 2004).

The New Health Privacy Rule, effective April 14, 2003, has made it illegal for healthcare providers and insurers to release a patient's medical records without the individual's consent (Cropper, 2001). Rule provisions dictate that healthcare providers and insurers must have a written information security policy and present it to patients (Cropper, 2001).

The objective of this study was to examine the effectiveness of an information security policy in influencing the reporting of both computer abuse incidents and the associated seriousness of those incidents. The detection and reporting of computer abuse incidents is the beginning of any enforcement practice which is a potential topic of further research. The beneficiaries of this study are especially the health care industry, other industries in general, federal and state legislators, and researchers as these entities seek to identify and implement methodologies to safeguard information.

Review of the literature

Prior to formalizing the model used to investigate the importance of information security policy, a comprehensive literature review was conducted. The issue of information security has received considerable attention from both academics and practitioners. The general topic contents of prior studies that addressed information security can be classified as: definition of what is at risk, definition of information security and computer abuse incidents, threats to information security, risk analysis and assessment, defense measures, and concerns and responses to personal information security.

When examining these general topics, it is also necessary to understand the nature of computer abuse. For purposes of this study computer abuse is defined as the unauthorized, deliberate, and internally recognizable misuse of computers of any organization's information system by individuals (Straub and Nance, 1990). Possible violations include:

(1) The unauthorized access of a computer to obtain information relating to hospital operations, to obtain information relating to hospital financial records, or to manipulate information on a computer that would adversely affect the hospital's operation of the computer.
(2) Accessing a hospital computer without, or in excess of, authorization and with intent to defraud or obtain anything of value, to include medical record information.
(3) The intentional access of a hospital computer without authorization, where such access alters, damages, or destroys information, to include medical records, or prevents ''authorized use'' of the computer.
(4) Certain types of reckless conduct in addition to intentional acts. This may include the transmission of malevolent software, such as computer viruses, if such actions are sufficiently reckless.
(5) Knowingly, and with intent to defraud, trafficking in passwords, which would permit unauthorized access to a hospital computer (Benson et al., 1997).

Even though the literature alludes to the importance of a security policy in deterring incidents of computer abuse, there is no known study that has addressed the actual effectiveness of a formal information security policy in the prevention of premeditated or accidental unauthorized disclosures of sensitive information.

Definition of what is at risk

Today's Information Economy focuses on the creation and dissemination of information rather than the production of goods and services (Hill and Pemberton, 1995). In this Information Economy, international competition has made an organization's proprietary information more valuable than ever. Proprietary economic information is defined by the Federal Bureau of Investigation as ''...all forms and types of financial, scientific, technical, economic, or engineering information including but not limited to data, plans, tools, mechanisms, compounds, formulas, designs, prototypes, processes, procedures, programs, codes, or commercial strategies, whether tangible, or intangible, and whether stored, compiled, or memorialized physically, electronically, graphically, photographically,