Information & Management 52 (2015) 123–134

Contents lists available at ScienceDirect

Information & Management

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

A system dynamics model for information security management

Derek L. Nazareth [a,*], Jae Choi [b,1]

[a] Lubar School of Business, University of Wisconsin-Milwaukee, P.O. Box 742, Milwaukee, WI 53201, USA
[b] Kelce College of Business, Pittsburg State University, 223 Kelce Center, Pittsburg, KS 66762, USA

ARTICLE INFO

Article history:
Received 13 February 2013
Received in revised form 15 August 2014
Accepted 24 October 2014
Available online 4 November 2014

Keywords:
Information security management
Security investment decisions
Simulation
System dynamics

ABSTRACT

Managing security for information assets is a critically important and challenging task. As organizations provide clients with ubiquitous access to information systems and the frequency and sophistication of security threats grows, the need to provide security assumes greater importance. Effective information security management requires security resources be deployed on multiple fronts, including attack prevention, vulnerability reduction, and threat deterrence. Using a system dynamics model, this study evaluates alternative security management strategies through an investment and security cost lens, to provide managers guidance for security decisions. The results suggest that investing in security detection tools has a higher payoff than does deterrence investment.

1. Introduction

Information security remains a key issue in the IT industry, as indicated by recent surveys [54]. Security incidents continue to increase in frequency and sophistication [41]. As consumers push for greater access to data and applications in an increasingly connected world, the opportunities for security breaches will increase. Part of this growing awareness is reflected in the inclusion of security-related sections in IT publications and in the emergence of several new publications devoted to IT security. Though most organizations have taken a number of steps to fortify information security, it has been suggested that security investments are typically a response to perceived and materialized threats rather than a response to more rigorous analyses of the effectiveness of solutions in combating such threats [17]. Applying a cost-benefit approach to the problem is often not effective because many models tend to omit qualitative or nonfinancial criteria, which comprises a significant aspect of information security [9].

Information security managers are tasked with a variety of functions, including security planning, policy formation, staffing, risk management, security technology selection, threat assessment, countermeasure implementation, performance monitoring, and maintenance [73]. Selecting countermeasures to security threats remains one of the more pressing issues that requires attention on a continual basis. Managers can elect to counter a wide variety of security threats that are present with several strategies including detection, deterrence, vulnerability reduction, education and training. Clearly, a portfolio of strategies is preferred over the adoption of a single solution. Each security strategy entails different costs, effectiveness, and potential benefits; many of these are difficult to quantify. The business value derived from information security investment, although undeniable, may be difficult to estimate. This difficulty arises because of the uncertainties of threat manifestation, the extent of damage incurred, the ability to recover from successful attacks, any ripple effects to other parts of the business affected by a successful attack, and a loss of reputation. Many factors affect these assessments, including innate vulnerabilities, the perceived attractiveness of targets (both organization and individual application), the number and sophistication of attackers, the availability of attack tools and vectors, and the extent and nature of backup facilities.

Clearly, assembling an accurate business case can prove challenging. Nonetheless, information security managers need to select security strategies on a periodic basis. In the absence of adequate tools to support these decisions, managers will speculate about whether the decisions that were made were appropriate for the task. A model that captures the complexities of the security decision while permitting the systematic exploration of alternative security decisions would be an invaluable aid to managers. Using the design science research methodology [34], this paper develops a model that allows information security managers to examine the effects of alternative security decisions on the organization's information assets. Given the need to capture the dynamic and

* Corresponding author. Tel.: +1 414 229 6822.
E-mail addresses: derek@uwm.edu (D.L. Nazareth), jchoi@pittstate.edu (J. Choi).
[1] Tel.: +1 620 235 4541.

http://dx.doi.org/10.1016/j.im.2014.10.009
0378-7206/

fluid nature of the problem and to revisit the decision on a periodic basis, system dynamics is chosen as the modeling environment. The model simulates the security decisions over a 30-month horizon and can be adapted and calibrated for different organization contexts.

The remainder of the paper is organized as follows. A review of the extant information security literature pertaining to simulating security decisions serves as the foundation for building the information security management model; this is presented in the next section. A dynamic model of the mechanics underlying the impact and implications of security attacks is assembled and presented thereafter. The model is used to examine the implications of alternative security investment strategies in a variety of scenarios. Research and managerial implications of the simulations are discussed. Limitations and future extensions complete the paper.

2. Review of relevant literature

Security in the information systems discipline has represented an area of interest for years, with studies appearing in mainstream Information Systems (IS) journals in the early 1990s [5,64]. Several aspects of security have been studied, including internal abuse [30,32,65], external attacks [57,72], acceptable use policies [56,61,63,71], computer crime [18,60], and password security [40,75]. Research in the field is clearly growing; a survey identified 240 security-related articles published in 10 leading IS journals in the period 2000–2007 [13]. Much of the research is directed at individual behavior and spans topics such as Internet abuse [47], compliance with organization norms, ethical practice regarding computers, and the effect of deterrence on user behavior [36]. Studies at the organizational level are comparatively fewer and are decreasing in frequency. Some studies describe the adoption of security technology and practices [46], whereas others address the difficulties in adopting security standards [59] and relying on traditional methods [58]. The relative paucity of firm-level research may reflect the reluctance of organizations to reveal information regarding their security procedures and breaches; hence, firms elect to avoid participation in security studies [44]. The most recent security study, which surveyed security personnel, indicated a drop in the number of responses and the response rate compared with prior studies [54].

A number of meta-analyses in information security have emerged [5,21,58,66] that advocate for a more holistic approach to addressing information security issues. These studies identify several areas for research in security, including the need for models to gain a better understanding of information security. Several different types of models exist in the information security discipline. These include formal models for access, economic models for security, and simulation models for gaining insight into the dynamics of information security; these models are briefly reviewed.

2.1. Models for information security access

Formal models for information security were proposed years ago [45]. These are usually grounded in military computing and typically seek to formalize the basis for protecting information and network assets through access and usage patterns. Among the early models of access was the Bell-LaPadula model [7], which sought to maintain the confidentiality of information through controlled access by assigning distinct security levels to people and assets. A slightly different set of security principles was adopted in the Biba model [8], which focused more on data integrity through the restriction of content accessibility and updatability. Formal models to access programs and other objects at the operating system level were also addressed [33]. In this extension of prior work, the ability to add and delete new assets and people and to alter current authorizations is considered from a security perspective. Adapting previous models for military computing security to corporate applications and rules to govern security was proposed in the Clark-Wilson model [15]. This approach expands the set of rules to address a more varied set of business transactions. A related problem involving the restriction of information in which conflict of interest and insider information issues arise was addressed through the Chinese Wall model [10]. The approach was initially designed for investment banking scenarios, although it has also been used in legal firms. Though these models are effective at formalizing and enforcing policy at an asset and individual level, they are of limited utility at the firm level. In an increasingly connected world, information security managers need to focus more on threats and countermeasures at the entire computing infrastructure level, rather than at an individual asset level.

2.2. Economic models of information security

Economists have examined the interplay between economics and security for a considerable period. However, the emphasis on the economic aspects of information system security has only recently gained more attention. Several streams of research are identifiable. One stream is devoted to the economic modeling of security investments using a net present value approach. Research in this area examines the effectiveness of optimal expenditure levels [28], risk management [35], and the rate at which certain types of attacks bypass the existing security mechanisms and cause damage [3]. A different stream uses classic economic analysis, adopting the utility maximization principle to derive optimal investment levels of a firm under a limited number of constraining conditions [26,38,39]. A variant examines the use of financial options to examine the effect of deferred security investment on security breaches [29]. Still other approaches utilize the principle of equating marginal financial benefits of information security to the marginal financial costs of such security [27]. A survey of economic models of information security is presented in [2], where models are classified based on whether they address vulnerabilities, privacy, security mechanisms, or incentives and deterrence.

Economic models of information security generally adopt a quantitative approach. However, security goes beyond that and typically includes qualitative and non-functional aspects. In an effort to include these aspects, some researchers have employed the analytic hierarchy process to combine quantitative and qualitative criteria [9]. These studies often adopt a static view of the information security problem. However, in actuality, information security is a complex system that embodies many closely coupled variables; it involves people, organizational factors, technology, tasks, and the working environment [11]. In addition, the security management system often involves multiple controls, including technical controls, formal controls, and informal controls [20]; these call for a more dynamic approach to modeling information security.

2.3. Dynamic models of information security

Whereas formal models of security provide guidelines for security policy development, and economic models provide guidance for investment in security, any attempt to manage resources to improve information security must entail an understanding of the dynamic aspects of security threats, countermeasures and an effort to prevent and recover from attacks. Multiple diverse factors and many dynamic relations are involved and must be investigated. The dynamic aspects of information security can be studied through queueing theory and simulation. The former offers closed-form solutions but is difficult to apply for large and complex systems; in addition, the restrictive assumptions of queueing theory may not permit the accurate modeling of the real-world phenomenon. Simulation offers the