Information & Management 51 (2014) 138–151

Contents lists available at ScienceDirect

Information & Management

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

Incident-centered information security: Managing a strategic balance between prevention and response

Richard Baskerville [a], Paolo Spagnoletti [b], Jongwoo Kim [c,*]

[a] Georgia State University, CIS Department, 35 Broad Street NW, PO Box 4015, Atlanta, GA 30302, USA
[b] LUISS Guido Carli, Research Center on Information Systems (CeRSI), Via G. Alberoni 7, 00198 Roma, Italy
[c] University of Massachusetts Boston, MSIS Department, 100 Morrissey Boulevard, Boston, MA 02425, USA

ARTICLE INFO

Article history:
Received 24 October 2012
Received in revised form 14 October 2013
Accepted 7 November 2013
Available online 19 November 2013

Keywords:
Information security management
Prevention paradigm
Response paradigm
Security balance
Case study
Incident-centered analysis

ABSTRACT

Information security strategies employ principles and practices grounded in both the prevention and response paradigms. The prevention paradigm aims at managing predicted threats. Although the prevention paradigm may dominate in contemporary commercial organizations, the response paradigm (aimed at managing unpredicted threats) retains an important role in protecting information security in today's dynamic threat environment. This study provides an overarching security framework that focuses on managing the proper balance between prevention and response paradigms. We conduct a comparative case study with three European organizations. This study analyzes and empirically confirms how and why organizations balance between their prevention and response strategies.

1. Introduction

Information systems security management is undoubtedly a critical activity in a world where computing is ubiquitous and information systems are interconnected globally. There are a number of widely subscribed management frameworks available to guide organizations in formulating and operating their information security efforts. These frameworks include the ISO standards (such as ISO 27001 [26]), COBIT [12], and PCI [41], which prescribe technical, formal, and information security countermeasures [1].

Many of these frameworks are universal in scope [45] and have foundations drawn from quality control principles, such as Deming's quality cycle of Plan-Do-Check-Act (currently prevalent in ISO 27001) and the Software Engineering Institute Capability Maturity Model (prevalent in COBIT). Such quality control frameworks have proved appropriate in the past because they are particularly valuable for routine security tasks that support measurement and historical comparison. They exploit the threat–control relationship in which a threat expectancy (i.e., a probability) is met with a control treatment.

This focus on controls and their performance represents a control-centered security management that has been fundamental in information security strategy for decades. The earliest information security management approaches simply selected controls from checklists, while later, more sophisticated approaches designed controls based on exposure and risk analysis [6]. Quality management invites metrics while a fixation on measurement highlights histories of common threats. As a result, management attention concentrates on preventing the continuation of these known threats.

Consequently, this prevention-oriented philosophy and its sets of predefined controls may be less ideal in the face of today's more dynamic threat environment. Although the quality of standardized controls has improved, attackers are mounting more unique and targeted threats: one-of-a-kind, customized attacks that bypass quality control cycles. These dynamic and sophisticated threats (e.g., Stuxnet and Aurora) are rising [2,13]. Sometimes known as Advanced Persistent Threats (APTs), targeted attacks, or simply Attack 2.0, these dynamic threats affected more than 20% of companies surveyed by the Computer Security Institute in 2010 and comprised 16% of data breaches in the 2012 Verizon survey [43]. At large companies, 50% of the data breaches were targeted attacks. The dynamic nature of threats is also reflected in the customization found in approximately one-third of the malware breaches reported in the Verizon survey [52]. Organizations increasingly face the need to discover new threats and new forms

* Corresponding author. Tel.: +1 617 287 7746; fax: +1 617 287 7717.
E-mail addresses: baskerville@acm.org (R. Baskerville), pspagnoletti@luiss.it (P. Spagnoletti), jonathan.kim@umb.edu (J. Kim).

0378-7206/$ – see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.im.2013.11.004

of attack [3]. As a result, it is becoming less feasible to estimate cyber security risk in real world control systems because the problem involves an unpredictable intelligent adversary and very complex systems [10].

This increasingly dynamic nature of information security may be reflective of the more general increasing presence of exceptional situations in business [44]. For example, mobile computing is evolving quickly with new network standards which, in turn, quickly and easily allow unexpected security attacks to happen [27]. In addition to the growing attack dynamics, the actions of even well-trained, loyal employees who do not behave according to security guidance represent dynamic security risks when their unexpected behavior leads to unreliable security management predictions [21]. For example, Java coding guidelines can subtly lead to unexpected behavior and ultimately to unexpected security vulnerabilities [33].

This increasingly dynamic security environment requires more response-oriented security in addition to the existing preventative frameworks. In this paper, we describe the necessary shift from a prevention-centered security framework to an alternative, broader information security management framework. This broader framework focuses on the balance between prevention and response across a pivot point embodied by security incidents. Prevention operates until the moment a security incident occurs. Afterwards, response operates. We describe three case studies that help explain how this incident-centered information security operates in practice.

2. Strategic security goals: reliability and validity

There are fundamental differences between management strategies of prevention and response. These different orientations are highlighted in the design thinking involved in management design [38]. The differences parallel the contrasting notions of reliability and validity that are borrowed from prediction in science. A reliable prediction is one that is known to have been correct in the past. A valid prediction is one that is correct for the present situation. Reliability is anchored in the past, while validity is anchored in the future. The concepts extend to relations with fundamental management strategy. For example, reliability is aligned with exploitation strategies, which capitalize on what organizations have learned to do well, while validity is aligned with exploration strategies, which capitalize on organizational abilities to search for new capabilities [36]. Such studies, in both design thinking and organizational strategy, advocate a strategic balance between reliability/exploitation elements and validity/exploration elements. From a management design perspective, organizations should operate with an ideal mix of reliable/exploitative processes while also preparing for new horizons with valid/explorative processes.

As illustrated below, these concepts operate ideally in information security management because they align well with preventative types of controls (which tend to be highly reliable and exploitative) and recovery types of controls (which tend to be highly valid and explorative). The use of both preventative and recovery controls is common in well-established security frameworks. For example, Parker [40] included prevention and detection/recovery in his five essential security functions. Another example is Denning [17], who used similar distinctions in her model of defensive information operations. Consequently, the strategic balance between prevention and recovery is often taken for granted.

As this paper proceeds, we will show how prevention principles and practices are paradigmatically distinct from response principles and practices. The term prevention paradigm refers to information systems security principles and practices in organizations that are intended to prevent security incidents from happening. The term response paradigm refers to such principles and practices in organizations that are intended to react to information security incidents that have happened (or are happening). While the two paradigms are complementary rather than independent, they represent two quite different strategies for managing security.

3. Incidents: the pivot from prevention to recovery

Effective security policies and the enforcement of the security operations are quite different in fundamental ways between the two paradigms. With regard to the management of information security, managers need to strategically balance security operations across both paradigms depending on the organizational context. The quality management approaches that focus on prevention and control exploitation should be mixed with exploration and search approaches. It becomes necessary to rebalance security strategies across the two paradigms when the organizational threat context grows dynamic.

By centering information security management on the moment at which a fundamental security event occurs rather than on preventative control, management strategies can better address the balance between the two paradigms. While the notion of a security incident is one of common language, one formal definition reads, "a change of state in a bounded information system from the desired state to an undesired state, where the state change is caused by the application of a stimulus external to the system" [49, p. 18]. In other words, the moment-of-incident represents an event that evades any preventative controls – and the moment at which this event arises – and inflicts negative changes on information systems.

The moment-of-incident is the fulcrum of prevention versus response. It marks a time shift from a setting protected by deterrence and prevention to a setting modified by detected or undetected abuse [58]. The security incident incorporates both the incident itself and the discovery of it. If a threat is known in the past, principles of reliability and exploitation can be applied in management processes to deploy controls to prevent damage from the threat. The prevention paradigm is mainly left-of-incident on a timeline. If a threat is new and unknown or unexpected in the past, principles of validity and exploration must be applied in management processes to deploy controls to respond to the damage from the threat. The response paradigm is mainly right-of-incident on a timeline. See Fig. 1.

Primarily basing information security management on quality management and prevention principles (reliability and exploitation) is a good strategy when the threat environment is stable and recurrent. However, when this environment becomes less stable and dynamic, threats become novel, and the quality principles are overtaken by the need for response strategies (validity and exploration).

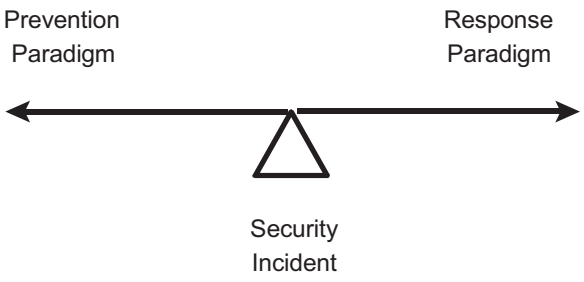

Fig. 1. The strategic incident lever from prevention to response.