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 LISS Guido Carli, Research Center on Information Systems (CeRSI), Via C. Alberoni 7, 00198 Roma, Italy
c University of Massachusetts Boston, MSIS Department, 100 Morrissey Boulevard, Boston, MA 02425, USA

A R T I C L E   I N F O

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

A B S T R A C T

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.

© 2013 Elsevier B.V. All rights reserved.

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
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/exploitation elements. From a management design perspective, organizations should operate with an ideal mix of reliable/exploitive processes while also preparing for new horizons with valid/exploitative 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.](image-url)
Table 1
Features distinguishing prevention models from response models.

<table>
<thead>
<tr>
<th>Features</th>
<th>Prevention paradigm</th>
<th>Response paradigm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assumptions</td>
<td>Threat tempo, Control tempo, Threat–control timing, Threat forecasting, Threat measurement, Threat–control logical form</td>
<td>Information systems security threats are persistent, Effective information systems security controls must be persistent, Threats and controls share a static relationship, Threats are predictable, The relationship of controls to threats is determinate</td>
</tr>
<tr>
<td>Logical structure</td>
<td>Causal structure, Unit of analysis, Safeguard–risk reduction definition, Relationship to time, Logical form, Ideal criterion, Strategic goal, Learning strategy</td>
<td>Variance, Variables, Safeguard is necessary and sufficient to reduce risk, “IF X then Y”, Reliability, Quality, Exploitation</td>
</tr>
<tr>
<td>Organizing principles</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Adapted from [8].

4. The contrast between prevention and response

The distinction between prevention and response should not be taken for granted as simple or unimportant. For example, computer virus defenses have long been modeled on the epidemiological notions of inoculation and recovery [31]. Nor are response and prevention activities mutually exclusive. Response technologies, such as intrusion detection do not eliminate the need for prevention technologies, such as password access controls [20]. Prevention and response efforts must be balanced for the security situation at hand. Too much emphasis on prevention mechanisms implies an insufficient development of response mechanisms [28]. On the other hand, emphasis on prevention should not be lost entirely. For example, time-based security prevention is a primary warning mechanism. Where time is a primary measure of risk, security is obtained through advance warning. Security exists when advance warning time exceeds the sum of detection and response times [9]. It is important to understand the fundamental differences between prevention and response models of security.

Prevention models operate by looking across past experiences with known threats and estimating future occurrences based on continuing similar events. To prevent an event from occurring, it is first necessary to develop some evidence about these past events. Prevention invokes prediction, forecasting or estimations of the nature and likelihood of an event based on evidence from previous incidents [5]. Risk analysis, one of the most fundamental of all security management techniques, usually involves quantification of probabilities of a loss event based on past experience and, similarly, the costs of the loss associated with that event [7]. Prevention mainly involves control actions to be taken now, before the next predicted event occurs.

Response models involve planning for actions that mainly take place in the future. The idealized examples are disaster recovery or business continuity planning. Response models incorporate preparations for unknown, unexpected or unpredictable threats that may never even occur [30]. Response models may involve detection processes to identify when a security loss event has occurred [56]. Response models primarily prepare for quick and effective reactions to new types of events. A key characteristic of response is agility [18]. Response mainly involves preparing for control actions to be taken in the future – after an unpredictable event occurs [15]. As such, the diversity of these responses is wide. For example, responses can include forensics examinations and document retention activities for the purpose of legal discovery [55]. In response situations, the development of a formative context in which learning and innovation are favored can provide management with new capabilities to cope with unpredictable threats [48].

Prevention and response models for security events are not mutually exclusive and may even be interchangeable to a certain extent. For example, if risk analysis indicates that an event is highly improbable, the organization may decide to forego the expense of operating preventative controls and self-insure against the risk. However, the organization may instead explicitly substitute the detection and recovery of such an unexpected event in its incident response planning because having no recovery policy would place the organization in jeopardy.

Because prevention and response models are fundamentally different approaches to the achievement of information security, we need to understand precisely the strategic difference between response and prevention. Table 1 details differences in the assumptions, logical structure, and organizing principles between prevention and response models. The details of the differences highlighted in Table 1 are elaborated in the next section.

4.1. Prevention paradigm

The prevention paradigm shown in Fig. 2 entails three essential assumptions about security risks that give rise to two further assumptions about the risks–safeguards relationship [8].

4.1.1. Assumption 1: predictable risks

The prevention paradigm assumes that risks are predictable. This assumption is evident in risk assessment and analysis
methods, such as cost-benefit analysis. Such methods start by listing an inventory of information systems assets and corresponding threats to each system asset [34]. Without the assumption that risks are predictable, analysts cannot formulate such an inventory of threats. Afterwards, to assess threats to each asset in an information system, security analysts would predict a level of existing threat for each asset. This process leads to the second assumption about risk measurability.

4.1.2. Assumption 2: measurable risks

Predictable risks mean that we can necessarily state the existence of these risks. Therefore, at least binary measurement of risks is assumed. Furthermore, most risk assessment methods provide detailed scales and measurement items, although many of them are estimates. Along with such risk measurements, expected loss/cost amounts also often populate measurement tables.

4.1.3. Assumption 3: persistent risks

The prevention paradigm assumes that risks are persistent. It presupposes that inside/outside attackers are constantly attempting to compromise organizational information systems. Information security legislation and standards reflect this assumption [14], often prescribing vigilant and constant safeguards to cope with such persistent risks. Examples of safeguards implied by this assumption are intrusion detection and prevention systems.

4.1.4. Assumption 4: static relationship between risks and safeguards

The prevention paradigm views the relationship between risks and safeguards as static to a large degree. To counter persistent security risks, security safeguards with the same persistence should be deployed. The values of security safeguards that come from the persistence of risks are more or less constant. This statement means that the relationship between risks and safeguards is determinate. Security analysts can determine safeguards that will provide effective future protection against threats. In other words, security results can be determined in advance according to the deployment of security safeguards.

4.1.5. Assumption 5: the logic of prevention

Variance theories are the logical foundation of the prevention paradigm approach. Variance theories assume a causal relationship between predictor and dependent variables. According to variance theories, the level of a predictor variable can determine the resulting level of a dependent variable [37]. Examples of this logic take the forms of “if X then Y” and “if more X then more Y”.

4.1.6. Single-loop learning

The prevention paradigm often adopts a mode of organizational learning described as single-loop learning. This mode assumes that problems and their solutions are close to each other in time and space [4]. In this form of learning, people primarily consider their specific actions instead of the governing principles or context of those actions. Small changes are made to specific practices or behaviors that are based on what has or has not worked in the past. This process involves doing things better without necessarily examining or challenging underlying beliefs and assumptions. The goal is improvements and fixes that often take the form of procedures or rules. Single-loop learning leads to making minor fixes or adjustments, such as tweaking a firewall configuration to control network access.

4.2. Response paradigm

The response paradigm shown in Fig. 3 also entails three contrasting essential assumptions about security risks that give rise to two further contrasting assumptions about the risks-safeguards relationship [8].

4.2.1. Assumption 1: unpredictable risks

The response paradigm assumes that risks are often unpredictable. Successful attacks are designed to take defenders by surprise and overwhelm any defensive safeguards that have been deployed. Examples include the Attack 2.0, APT, or dynamic risks described earlier. Threats are customized and largely difficult to assess in advance. Therefore, defensive operations should prepare for unexpected and unpredictable risks.

4.2.2. Assumption 2: non-measurable risks

Risks cannot be measured because they are unpredictable. Estimating risk levels is not possible when risks cannot be

<table>
<thead>
<tr>
<th>Table 2</th>
<th>Summary of cases.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RAIL</strong></td>
<td><strong>ROYALPOL</strong></td>
</tr>
<tr>
<td>Value proposition</td>
<td>• Rail transport services</td>
</tr>
<tr>
<td></td>
<td>• Logistics</td>
</tr>
<tr>
<td></td>
<td>• Railway infrastructure management</td>
</tr>
<tr>
<td></td>
<td>• Railroad stations management</td>
</tr>
<tr>
<td>Organizational structure</td>
<td>• Private group (11 companies)</td>
</tr>
<tr>
<td></td>
<td>• 80k employees</td>
</tr>
<tr>
<td></td>
<td>• 3k railroad stations</td>
</tr>
<tr>
<td>IT and security governance</td>
<td>• IT infrastructure outsourced: central IT Department in charge of contract management</td>
</tr>
<tr>
<td></td>
<td>• Information security managed in the Corporate Protection Department of headquarters</td>
</tr>
</tbody>
</table>
predicted in advance. This statement is especially true when we cannot state the existence of risks. Therefore, even the simplest binary measurement of risks is not possible.

4.2.3. Assumption 3: transient risks
The response paradigm assumes that risks are transient. This assumption means that attacks are innovative and unexpected, aiming to take defenders by surprise. Attacks focus on the area in which defenders are poorly prepared. Attacks cannot be routine as defenders will be ready for such attacks. However, attacks can be repeated when attackers find that defenders have ignored history and remained unprepared.

4.2.4. Assumption 4: dynamic relationship between risks and safeguards
The response paradigm views the relationship between risks and safeguards as dynamic to a certain degree. To counter transient security risks, security safeguards with the same transience should be deployed. Bricolage, hacking, and improvisation capabilities must be cultivated within inter- and intra-organizational formative contexts [48]. Effective security measures should be agile because the risks are unexpected and unique. Organizations should respond to newly detected and unique risks by rapidly deploying customized safeguards. The relationship between risks and safeguards is not only dynamic but consequential. Safeguards become a consequence of innovative and transient risks. The basis for defensive information operations is an agile process of rapidly developing innovative, new safeguards rather than persistent safeguards. Defensive information operations focus on how to develop and deploy safeguards quickly to respond to unexpected and transient attacks.

4.2.5. Assumption 5: the logic of response
Process theories are the logical foundation of the response paradigm. Process theories do not assume a causal relationship between predictor and dependent variables. Instead, the predictor is assumed to be insufficient but necessary to cause the outcome [51]. The outcome may not occur even when the conditions are present. The logical form of process theories is “if not X then not Y” and does not imply any relevance of “more X” to “more Y”.

4.2.6. Double-loop learning
The response paradigm often adopts a mode of organizational learning described as double-loop learning. It assumes that the organization must examine and alter the governing assumptions and hypotheses to find a solution to a problem [4]. Double-loop learning leads to insights about why a solution works or does not work. It is related to major fixes or changes to solve complex security problems. Double-loop learning is relevant to decision-making skills, which result in changing the underlying governing variables, policies, and assumptions.

4.3. Time continuum

Fig. 4 provides an overview of the prevention and response paradigms in relation to security incidents. It elaborates Fig. 1 by framing the moment of an incident with concepts from defensive information operations [17] and incorporates the timeline suggested by an extended security action cycle [57]. The security moment-of-incident is centered in the framework. Time before the incident grows to the left (known as left of bang). Time after the incident grows to the right (known as right of bang) [57]. The left side of the incident is dominated by the prevention paradigm, whereas the right side of the incident is dominated by the response paradigm.

Both paradigms connect in proactive and reactive ways. The left-of-bang prevention paradigm is mainly proactive in the sense of predicting measurable risks and preventing them with proper warnings and safeguards (e.g., intrusion detection system, security policy and regulation). The prevention paradigm connects to
incident response reaction by benefiting from hardened resources against future attacks. New preventative deterrence also proceeds from reactive lawsuits, prosecution or retaliation. Preventative measures benefit from learning about past attacks and better-formulated policies that deter or prevent repeat attacks. However, instead of focusing on a rapid response to unavoidable attacks, the prevention paradigm focuses on reducing future occurrences of the identified security weaknesses. For example, new signatures of attacks are identified and updated to security equipment regularly.

In contrast, the right-of-bang response paradigm is mainly reactive in detecting unexpected and unpreventable security breaches and responding to them. Such responses confirm that incidents have occurred and operate in agile ways to recover from them. The recovery may include investigations and lawsuits. The response paradigm also connects to incident prevention proactively by developing and deploying innovative new safeguards that quickly harden resources and develop organizational learning for preventing and deterring attacks, such as developing security policies and regulations. However, instead of focusing on predicting and preventing attacks, the response paradigm focuses on detecting losses and reacting quickly, efficiently, and effectively in recovering from the attacks.

The prevention paradigm and the response paradigm do not operate in isolation. The changing intensity of the graduated shading on the left and right side represents this changing isolation as the timeline approaches and departs the moment-of-incident in Fig. 4. Organizations should avoid having an over-simplistic point of view regarding the relationship between these two paradigms because the two paradigms supplement, connect and interact with each other rather than being mutually exclusive. The relationship embodies organizational learning theory within the context of security management. Once a new attack occurs that circumvents existing preventative security management, a double-loop style of learning proceeds that questions established security safeguards and their assumptions. New preventative safeguards may be developed (as well as new response processes). When organizations are similarly attacked in the future, a single-loop style of learning proceeds to refine and improve preventative safeguards until another event overpowers preventative safeguards and triggers the double loop again.

An organization can strategically view and implement information security features with differing weights on each of the paradigms depending on their situation. We may speculate that the prevention paradigm has been more typically dominant in commercial organizations. A stable security environment in which resources are readily made available and persistent/predictable attacks are launched would reward exploitative and reliable strategies such as preventative security. We may also speculate that the response paradigm has been more typically dominant in military organizations. An unstable and dangerous security environment in which resources have been withheld and non-persistent/unpredictable attacks are attempted [32,39] would reward exploratory and valid strategies such as responsive security.

Of course not all commercial organizations operate in stable security environments nor do all military organizations operate in unstable security environments. Even where one security paradigm is dominant, both paradigms are likely to be present, but unequally weighted in the strategy. For example, commercial organizations with reasonably stable security environments may still prepare a disaster recovery plan and a business continuity plan, which indicate the presence of the response paradigm. These plans protect the organizations from potential risks, which cannot be removed completely. Commercial organizations with less stable security environments may promote agile response capability to security threats. New security threats, such as worms and viruses, can spread rapidly across organizations. A rapid distribution of a new security patch is based on the premises and principles of the response paradigm. Military organizations may also deal with stable and unstable security environments and may use preventative security measures that represent the prevention paradigm. For example, even military information systems will need standard preventative measures, such as access control and backup practices.

Any past, general distinctions between military and civilian strategies amongst these two paradigms are unlikely to endure much longer. Many factors serve to decrease the stability of commercial information security environments, including the ubiquity of information technology and the integration of military purposes into civilian information systems, which makes these systems legitimate targets for information warfare [29].

5. Research methodology

Based on the incident-centered security framework developed above, we conducted a comparative case study to investigate how and why organizations adopt and configure their prevention and response information security management practices. The purpose of the case study is to empirically confirm that the framework describes information security management features in practice, develop insights into information security management approaches based on the framework, and determine the possible practical value of the framework for setting future organizational security management practices.

Case studies can provide rich descriptions of a phenomenon and also provide understanding by allowing in-depth analysis by researchers [53]. Multiple cases offer investigators a deeper understanding of processes and outcomes and provide a good picture of locally grounded causality [59]. One established tactic is cross-case comparative case studies. This approach permits investigators to select categories or dimensions (such as those belonging to our incident-centered security management framework, and including the distinction between the prevention and response paradigms) and look for similarities and differences within and between cases [24].

5.1. The cases studied

Given the contingent nature of the relationship between information security management practices and the internal and external organizational contexts, we identified three organizational profiles that, despite some structural similarities, are quite different in terms of the environmental conditions in which they operate. This difference allows us to achieve a theoretical replication logic by predicting contrasting results for anticipative reasons [59, p. 54]. The first profile corresponds to an organization operating in a stable commercial environment. The second profile corresponds to an organization operating in a warfare setting. The third profile corresponds to an organization operating in an environment in which the former and the latter settings are mixed.

Three organizations have been selected on the basis of their fit with these profiles and their willingness to support the research. The incident-centered framework is used as a lens to comparatively analyze organizations’ approaches to information security management and explore how and why they adopt different security practices in their environment.

The three cases involved large organizations with different scopes and purposes, yet possessed sufficient common characteristics to comparatively analyze their approaches and practices on information security management. All three organizations operate in the same European country and have a similar number of employees (approximately 100,000 each), a
nationwide geographical coverage of operations, a capillary distribution of subsidiaries across the country (approximately 10,000), and a long historical tradition (more than one century). These structural and historical similarities are complemented by differences in terms of the external environment in which they operate, their organizational goals, their processes, and their culture. The first organization (RAIL) manages the nationwide train and railroad system. The second organization (POSTAL) is the main postal service provider and delivers additional services, such as banking, insurance, and mobile services. The third organization (ROYALPOL) is a military force with police and law enforcement functions.

5.2. Data gathering and analysis

Our primary source of data includes interviews and documents on the organizational environments and information security management practices. We used documents to corroborate and clarify the data collected through interviews. The use of multiple sources of information helps demonstrate the credibility and dependability of interpretive case study research [16,59]. We developed a semi-structured interview guide (see appendix) and conducted interviews with senior information security managers. The managers we interviewed were key decision-makers and the most knowledgeable professionals in managing information security at their organizations. One of the authors conducted the interviews and met the interviewees multiple times in late 2011. The interviews lasted between 60 and 90 min and were recorded and transcribed later. Afterwards, the transcripts were sent to the informants for review.

The data were then analyzed interpretively using the incident-centered security framework [54]. We color-coded the interview data to identify concepts drawn from the framework. The coded text fragments from the interview transcripts were tagged, along with justifications for the selection. The interviewer's familiarity with the companies may have impacted the quality of the data collected. To minimize the possibility that the interviewer's perspective might jeopardize the validity of the analysis, all three authors analyzed data separately and developed a consensus on the analysis.

The case studies were used in more than confirmatory ways. Certain concepts, such as the double-loop learning phenomenon, arose from the case studies and were used to improve the fidelity of the incident-centered framework in comparison with the actual case phenomena.

6. Comparative case study

6.1. Case one: RAIL

RAIL is a large holding company that includes approximately 40 subsidiaries. The most important companies in the group operate rail transportation systems. The remaining companies provide internal services within the group (e.g., financial, engineering). Within the Corporate Protection area, the Chief Information Security Officer (CISO) is mainly responsible for managing new information security projects, outsourcing contracts, disaster recovery and business continuity issues for the whole group. Other departments in the same area are in charge of the surveillance, physical security and general protection of the railway infrastructure. The duties of the IT Department of each company are limited to the definition of functional requirements for new IT projects, while project execution is allocated through tenders.

Information security management is a complex issue because RAIL performs many diverse and unique industrial processes throughout the national territory. Accordingly, the IT infrastructure management is outsourced to a leading global service provider of enterprise security solutions.

6.1.1. Prevention and response paradigms at RAIL

Not surprisingly for a large commercial company, the adherence of the RAIL information security strategy to the principles and practices of the prevention paradigm is prominent. The main security concerns relate to IT governance in a complex business environment where the deployment of new systems must take into account the variety of the existing infrastructure (i.e., legacy systems), differing functional needs, and local office budgets. Central elements of the information security management include the standardization of project implementation and delivery, the efficient allocation of resources, and the prioritization of security issues through risk analysis.

“All approaches must be homogeneous, from the business impact analysis to the implementation and delivery of a company's project. All the issues related to the governance of these large industrial groups are crucial: some IT processes may get out of hand and lead to an increase of expenditure. For instance, in making the workstations secure for users, as well as in office automation, the company has found that there were thousands of different software programs in use. Even if well planned and assessed, only 90% of workstations can be secured. For the remaining legacy workstations, the company found that it was more convenient to build and secure new workstations than develop and apply security measures to legacy ones.”

In this context, availability, integrity, and confidentiality issues can be identified and risks can be calculated and managed through safeguards. For instance, the security management team has estimated that the expected losses from the unavailability of the online ticketing system on a Wednesday afternoon are approximately €800,000. Furthermore, integrity violations related to rail schedule problems and delays trigger sophisticated passenger safety measures based on mechanical controls. Confidentiality issues are crucial because the company also deals with the transport of “dangerous material” (e.g., government, military).

Such aspects depend on the nature of both the environment and the resources through which RAIL operates and require the timely adoption of state-of-the-art practices for managing information security. RAIL takes pride in its highly regarded information security certificates, and requires similar excellence in its service providers. To achieve an adequate level of agility in incident detection, the organization employs a Service Level Agreement (SLA) with the outsourcer that requires recognition and analysis of an anomaly within 20 min maximum and the identification of a security incident with a minimum accuracy of 98%. Although most of security management is outsourced, RAIL manages the security of the most critical systems (e.g., its ticketing system) internally.

“RAIL is really mature in terms of security. Since 1999, one of the most important companies of RAIL has certified its Information Security Management System (ISMS) with the BS7799 standard [50]. For many years the perimeter of this certificate has represented the largest in the world with regard to rail traffic information systems. Now the certificate has been updated to the new version of the standard (i.e., ISO 27001) and it is still among the largest in the world.”

Because RAIL business processes are tightly linked with its outsourcers, the perimeter of the information security management system extends to these business partners. This inclusion is an ongoing process related to semantic and organizational interoperability.
The prevention paradigm is dominant at the core of the information security strategy of RAIL. RAIL mainly perceives risks as predictable, provided an appropriate qualitative and quantitative risk analysis can be conducted. Furthermore, RAIL perceives risks as measurable and persistent because the relationship between risks and safeguards is considered static and determinate.

"Where the process is mature, it is easier to develop prevention, since process knowledge and statistics are available. . . . (Risks) may be converted into measurable risks through a risk analysis (mainly qualitative and subjective), which allows us to better understand the assets and processes involved. . . . Prevention implies technological developments, process innovation, and so on. . . . We adopted an anti-Denial of Service system which has been for many years the first in Europe . . . Even considering the evolution of the InfoSec threats, risks are perceived as persistent."

Although there is a bias toward the prevention paradigm, RAIL also acknowledges that conducting risk analysis is not an easy task and that it is not possible to prevent all types of risks.

"Even the best plan may not hold the impact with the enemy . . . . There are areas where talking of prevention does not make any sense . . . . The plurality of the industrial processes is the company's Achilles' heel . . . . The organization is able to say where it is able to prevent and where not . . . . Of course they (Risks) change. They are strictly related to the evolution of the company, its core processes, and so on. Furthermore there is an evolution of the threats which are outside the organization. Even technology has a deep impact on them both internally and externally as an environment element."

In these cases, risks are perceived as unpredictable, non-measurable, and transient. Their relationship to safeguards is dynamic and consequential. In fact, countermeasures reflect these assumptions and focus on incident response management, contingency plans, business continuity, and other proactive measures.

RAIL's management of information security reflects a management principle that makes passenger safety the top priority. When incidents occur, the main objective for RAIL is to return to the status quo as soon as possible. The dominant context of information systems switches from performance to control for passenger safety. For example, when abnormal system actions are detected, blocking Internet traffic from certain sources is allowed.

Once the incident has been identified, either single-loop or double-loop learning is activated. For a minor security incident, compliance with policies is verified, and relevant business processes are improved. Double-loop learning is activated following serious incidents, and the outcome is a disruptive change in the overall security strategy.

"[When incidents are detected] an ad-hoc committee immediately meets. The committee members include the CIO and business manager at the subsidiary company, the director of Corporate Protection at RAIL, and myself who are responsible for the incident management unit . . . . In addition the regular committee meets each month."

The ad-hoc committee met three times following serious incidents in the past. When the serious attacks occurred, the committee led the company to "wake up" and fundamentally review its security measures. While minor incidents served as a "stimulus" to improve existing security management practices, serious incidents led to a change in the governance structure of information security that centralized the responsibilities at the holding level. After a serious security incident in 2010, RAIL defined new security requirements and expanded the outsourcing contract.

"Individual companies must not deal with software development, but exclusively with the design of those information security requirements . . . . The management of information security then disappeared at each company. It went back to the parent company . . . ."

A tension between the actual practices and the individual position of the interviewee emerges even as RAIL balances the two approaches of information security management through its outsourcing contract. For example, RAIL fails to engage in community efforts to share its security practices and experiences with other organizations.

"RAIL does not participate in security communities (I personally consider this as a weakness). Even in recent years, it has been reluctant to show itself and share information in meetings and conferences (apart from some connections with the academia)."

6.1.2. Insights from incident-centered analysis

By analyzing the information security strategy of RAIL through the lens of the incident-centered framework, a number of important elements emerge from the case. First, RAIL's security management primarily focuses on prevention. It is also aware of the limits of prevention approaches. Second, service providers play important roles in the detection of security incidents. SLAs with outsourcers represent the organizational leverage for enhancing the level of organizational agility in the management of information security. Third, serious security incidents activate double-loop learning in which the overall information security management structure is re-designed by means of disruptive changes in roles and responsibilities. Finally, to recover the control of information management in security incidents, RAIL is willing to compromise its performance by slowing down operations. Consequently, bricolage, improvisation and hacking capabilities are enacted to design an ad hoc solution [48]. This behavior is borrowed from the organization's century-long experience in passenger safety practices. RAIL manages its security through outsourcing except for its core security management. It does not participate in security communities to share security information.

6.2. Case two: ROYALPOL

ROYALPOL has a long tradition of serving as both a military force and a law enforcement agency. This function means that all of its employees are civil servants and subject to military rules. The organizational structure reflects these military characteristics. A well-defined hierarchy among units with different ranks allows for centralized control of operations from the headquarters. In this way, orders flow rank-downwards and information and requests rank-upwards from approximately 5000 subsidiaries layered in five levels. The organizational unit in charge of IT governance is located in the headquarters. This unit hierarchically controls a network of IT officers and agents who are spread across the subsidiaries. Moreover, a large number of IT specialists operate in the headquarters offices. In this context, the Information Security (InfoSec) Department is in charge of both protecting all critical areas and reacting to both old and new vulnerabilities.

As a military organization, ROYALPOL's approach to information security management is mainly conservative and characterized by a degree of organizational inertia [35], with the exception of a few highly advanced divisions. The InfoSec unit plays the role of gatekeeper within the organization's hierarchical network. It supervises both the design of new systems and the monitoring of system usage.
6.2.1. Prevention and response paradigms at ROYALPOL

The military nature of ROYALPOL leads it to strike a balance between the two paradigms in a unique fashion. ROYALPOL enforces the maximum level of the response paradigm. Recovering its information systems with agility and effectiveness is its utmost priority when they are compromised by unpredicted security threats. ROYALPOL has many resources to implement this practice. For example, ROYALPOL engages in the prevention paradigm by protecting its information systems in a conservative way. It erects many preventive measures against different types and levels of risks even without conducting risk analysis in advance. In addition, ROYALPOL minimizes access to its information systems by all ranks of officers. In this way, preventive measures are implemented in daily regular operations. This approach has been so successful that ROYALPOL has not experienced any serious security compromise to date.

“As a military, quite conservative organization, the InfoSec Department aims to protect all critical areas and react to both past and new vulnerabilities. . . . we are concerned in supervising not only the design of a new project or system . . . (but also) in reacting to both past and new vulnerabilities. . . . In this phase (IT system usage) indeed security attacks more likely occur. . . . information leakage is the main concern. . . . given the importance of the information gathered, ROYALPOL is aware that a breach in its own IS would mean a disaster not just to the organization itself, but even to other organizations and the entire country.”

In the military context, risks are mostly assumed to be unpredictable and non-measurable. Each information asset represents a source of potential weakness. There are no metrics for risk assessment. Risks are everywhere, and it makes no sense to prioritize them according to the probability of occurrence. The ROYALPOL case confirms these assumptions.

“Unpredictability is linked to the so-called “related information” . . . The more a risk is “old” and known, the more it might become dangerous since it is no longer the center of discussions and controls for the scientific community . . . all the information ROYALPOL manages is extremely sensitive.”

The IT infrastructure is designed with the main purpose of creating a “wall” between the internal and external information systems. Given the presence of this physical and logical barrier, ROYALPOL can focus on the monitoring and detection of anomalous behaviors on a restricted set of entry points. Here, the metaphor of a “barricaded castle” can provide an understanding of ROYALPOL’s security approach. Implementing the maximum level of prevention within the walls and focusing on reaction to internal and external attacks is the information security strategy at ROYALPOL.

“Information may be sensitive or not sensitive. The most critical information is put in the safest areas of the intranet. This guarantees the integrity and safety of the data. Within the organization, a strict control of information security is maintained. . . . from the outside to the inside, the email is considered the most dangerous kind of communication too.”

There is tension between the need to innovate and the need to preserve the current security management approach. ROYALPOL is aware that innovation would enable better communication and collaboration among employees. Nevertheless, the military context of the organization and the nature of the information gathered do not allow innovation to be a top priority. ROYALPOL perceives that innovative information systems may entail unexpected security holes in its information system, which has been protected successfully. However, the interviewee notes that ROYALPOL’s security approach could be improved by developing new capabilities to assess the risk.

“I hope to embrace a more scientific approach as soon as possible. OSSTMM [25] is the last standard followed: this simply provides numeric values that are a function of the risk exposition, the adopted safeguards, etc. So far this is the only way that leads to a measure based on a number . . . Unfortunately it [security focus] has never changed . . . By the way, it must be said that nothing serious has happened so far.”

With respect to the response to a security incident, the approach is to face the problem through collaboration between the security team and the available organizational resources at all levels. Actually, there is no detailed recovery plan, but a disaster recovery site has been implemented for ensuring the availability of an alternative IT infrastructure. No tasks or responsibilities are assigned in advance. ROYALPOL has not experienced any serious attacks on its information systems thus far. Nevertheless, some examples of single-loop learning have been noted following incidents in peer organizations.

“Security incidents may be so many and different that it would be impossible to write down a recovery plan for each one of them. . . . Generally speaking, ROYALPOL has not reported any incident which has required the adoption of new technologies or countermeasures. . . . Practical guidelines for the end users have been recently distributed as the result of a long debate fuelled by the incidents occurred to peer organizations.”

6.2.2. Insights from incident-centered analysis

The sensitivity of information makes many risks predictable and measurable with the maximum level of severity control. In this highly sensitive military context, each new risk is considered as persistent when it is first identified. Second, the maximum level of safeguards is implemented through physical and logical barriers while minimizing the points of access to the information system. A response approach is applied to both old and new threats through slack resources, which operate constantly in a warning state. When the response paradigm prevails in organizational security management, a conservative and fine-grained approach may be adopted for the prevention paradigm. It is an interesting state in which the response paradigm has the major focus of management, and the prevention is nearly unmanaged because all preventative measures are simply taken by default. Such an over-engineering of prevention may have an unplanned negative impact on IT innovation.

6.3. Case three: POSTAL

POSTAL is the holding company of a group of companies that deliver a multitude of services all over the country, such as postal, banking, insurance, and mobile phone services. POSTAL had been a public organization providing traditional postal and bank services since the beginning of the 19th century. Due to the privatization of POSTAL approximately 10 years ago, the value proposition of the group has been completely renewed with the deployment of new business processes on top of the existing infrastructure of the old company. The adoption of innovative IT systems and the IT-business alignment are central elements of this innovation process. POSTAL continues to expand into different lines of business and continuously develop new applications.

The Business Protection Department at the POSTAL headquar ters oversees all security governance issues, including the strategic development and monitoring of internal policies and regulations. Therefore, the information security of each company is managed externally from the IT Department of POSTAL.
POSTAL plays a key role in actively promoting and supporting the exchange of information security practices through the development of a community of experienced practitioners that spans across organizations from different industries and several European countries. A European security task force initiated by POSTAL aggregates technical skills and expertise thereby providing a platform for the exchange of operational information. The task force provides organizations with a continuous update of security information so that they can update their security guidelines and policies. Furthermore, POSTAL has established a security control center with a group of approximately 40 employees who monitor information systems 24 h a day, these employees are ready to take appropriate actions immediately for any abnormal security threats.

6.3.1. Prevention and response paradigms at POSTAL

POSTAL operates in a complex and rapidly evolving environment in which competitive pressures determine the need to continuously update the company business model by adopting innovative IT solutions. As a result, the organization is continuously facing new risks. The management of information security focuses on the protection of a vast amount of resources (e.g., SIM cards, bank transactions, local agencies, national and international money orders, currency exchange services, and post office current and savings accounts). Other key issues for security management include complying with laws and regulations and preserving a trustworthy image with customers.

"Potential attacks and damage may be caused by external sources and by employees. … POSTAL is a continuously evolving structure, made of diversified and independent areas. … All these realities come to operate on different businesses, each of which involves different risks. … POSTAL keeps expanding into different lines of business and developing new applications. Of course new technologies, services and spaces bring new risks. Security risks are always around the corner. … This will bring the necessity of investigating all the aspects related to these new technologies such as private cloud … POSTAL cannot give up these business opportunities and be cut out of the market, but still cannot give up its security. … (Our) business information archives have significant value. If only someone had been able to tamper with them, certainly newspapers would have spoken at length about it."

In this context, the organization acknowledges that risks' predictability, measurability and persistency cannot be established a priori and homogeneously for all types of threats. A balanced approach to information security management is adopted. Regulatory compliance and security standards provide guidance for estimating risks and preventing losses. Risk assessment and business impact analysis are helpful in taking a snapshot of the organizational vulnerabilities.

"The information risk is perceived as very strong. A survey of all business information archives (which are some hundreds of thousands) has been made recently. Their compliance with the ISO 27001, the minimum requirements, and the privacy code has been verified. … Actual vulnerabilities have been studied and the impact of each of them has been assessed (business impact analysis)."

Nevertheless, risk assessment is considered to be a dynamic activity that copes with risks and vulnerabilities that are continuously changing their nature.

"Transient risks can definitely become persistent due to the evolution of technology, services, even internal processes and service delivery models. Risks change their nature. … Vulnerabilities change, as the technological scenario and the landscape of service delivery evolve, resulting in constantly updated and innovative products. Even the impact of each vulnerability changes. … Risks go along with the evolution of technology."

As a consequence of this dualistic view on the nature of risks, the relationship between risks and safeguards is also regarded as dynamic. The capabilities to actively monitor and react to threats are the key elements of security management.

"About responsiveness, there is certainly not a negligible effort. All transactions and related risks are monitored and analyzed. POSTAL has very sophisticated systems, a security control center, with groups of around forty people who monitor 24 h a day, 7 days a week, detecting all the anomalous accesses. When alarms switch on, accounts are locked and all technical actions are taken in order to protect the customers, interpret the abnormal signals and always have a ready answer."

As to the reaction to a security compromise, POSTAL adopts a two-step approach. The first step is an analysis of what happened. The second step is an ad hoc business continuity and resource recovery plan. A crucial issue in the second step is to understand the macro consequences of the attacks in order to react at appropriate levels.

"[S]ome years ago there was a website defacement: the web page layout had been modified, reporting these words: “This site has been hacked”. Just the layout had been changed: hackers hadn’t tampered with the corporate information archive. Nevertheless there was huge reputational damage. In that case the first thing to do was a first-level analysis of the macro impacts, then another, more detailed analysis about the countermeasures to adopt. Lastly there was a communication action, in order to make POSTAL’s stakeholders aware of POSTAL’s commitment.

The close collaboration with other companies, including POSTAL’s competitors, was the major change in response to security attacks to its systems. Before this event, POSTAL did not share its security information with its competitors. Afterwards, POSTAL exchanged security information (including best practices and past experiences) with other organizations. This collaboration enabled POSTAL to keep pace with innovation and to share critical security information.

"POSTAL organizes two to three hour security sessions where technical information about the dynamics of the incidents and new attacks are exchanged. It’s important to have the ability to always be on the frontier."

6.3.2. Insights from incident-centered analysis

The analysis of the POSTAL case viewed through the lens of the incident-centered framework provides the opportunity to capture multiple insights that can be summarized in five main points. First, the complexity and rapid evolution of the environment (i.e., market and technologies) force the organization to continuously face new risks. Second, the predictability, measurability and persistency of risks are so dynamic that they cannot be established a priori. Third, the dynamic relationship between risks and safeguards requires strong capabilities to monitor and quickly react to security incidents. Fourth, these capabilities are implemented through slack resources and the development of a formative context in which knowledge sharing with external organizations is encouraged. Finally, the double-loop learning activated by an incident supports a macro level view on the consequences of a security incident.
environment and manages information security as dominated by response (although without ignoring prevention). This strategy may be called a fat response strategy. POSTAL, at the bottom of the figure, operates in multiple types of security environments, some stable, some unstable, and manages information security as balanced somewhat evenly between the prevention paradigm and the response paradigm. This strategy may be called a balanced strategy. There is no one ideal or correct strategy. Each organization has adopted the best strategic balance for its own environmental setting.

Table 3 summarizes the insights from the three comparative cases. From each discussion, the table highlights the risk assumptions that the organizations are making about their environments, how this assumed environment affects the relationship between risks and safeguards, and why the organization has selected its strategic posture with regard to balancing their efforts in both the prevention and response paradigms.

Commercial organizations may face the need to make dramatic shifts in their information security strategic posture. In the past, they faced routine and predictable attacks for which preventative measures could be easily acquired and deployed. Moreover, there is increasing motivation to inflict more sophisticated attacks on information assets in commercial organizations [43]. The integration of civilian and military communication and information processing across the Internet (and in the cloud) makes many commercial systems legitimate warfare targets [11]. Additionally, the adoption of information warfare tactics between nation-states and non-state belligerents means that anti-commercial tactics may be deeply financed and intentionally aimed at bypassing known preventative controls. Aside from such APTs, financial attacks based on the compromise of individual assets have become sufficiently lucrative to attract new internationally organized crime syndicates [23]. Such attacks have grown in sophistication from phishing (mass emails intended to garner many small victims) to targeted spear phishing attacks (singular emails intended to mislead a specific and important victim) [13,46].

The comparative analysis of the three cases shows how organizations with similar historical traditions and dimensions but offering different service portfolios are taking three different approaches to the management of information security. While ROYALPOL, a public organization, is characterized by a greater inertia with regard to innovation and organizational transforma-

Table 3 | Insights from incident-centered analysis in the three cases.

<table>
<thead>
<tr>
<th>RAIL</th>
<th>ROYALPOL</th>
<th>POSTAL</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Risk assumptions</strong></td>
<td>- Risks are predictable, measurable and persistent when business processes are well known&lt;br&gt;- Aware of the limitations of risk analysis due to the complexity of internal processes and the relationships with external stakeholders (i.e., outsourcers)</td>
<td>- High sensitivity to risks makes ROYALPOL assume that all risks are predictable and measurable&lt;br&gt;- Each new risk is considered to be persistent as soon as it is identified</td>
</tr>
<tr>
<td><strong>Relationship between risks and safeguards</strong></td>
<td>- Use outsourcer to achieve agility in response to threats&lt;br&gt;- Double-loop learning leads to redesign of the information security strategy</td>
<td>- Maximum level of safeguards to information&lt;br&gt;- Quick reaction to both old and new threats&lt;br&gt;- Sufficient slack resources constantly in a warning status&lt;br&gt;- When the response paradigm prevails, a conservative approach in prevention has a negative impact on innovation&lt;br&gt;- Tension towards a fine grained prevention capability</td>
</tr>
<tr>
<td><strong>Balancing the prevention and the response paradigm</strong></td>
<td>- When security compromise occurs, a context is switched from performance to control&lt;br&gt;- Tension towards the development of a formative context</td>
<td></td>
</tr>
</tbody>
</table>

Fig. 5. Comparative security strategic balance between the three cases.
tion, RAII and POSTAL compete to provide better services to their customers than their competitors in the market. RAII’s value proposition focuses on the safe transportation of people and goods over a networked infrastructure of rails, railroad stations, and information technology. POSTAL provides a similar logistics service. However, the nature of the financial and mobile services provided by POSTAL requires a different infrastructure. Our data shows that POSTAL develops an information infrastructure based on an evolving socio-technical system of IT capabilities and modular applications to support its business and information security [22].

The balance of strategy in the cases may have also been related to the outsourcing/insourcing strategies made by the three organizations. While RAII is fully outsourcing its IT operations but remaining in charge of the policy definition and contract management, both ROYALPOL and POSTAL have chosen to internally manage their information security. In addition to such a simplified view of the outsourcing/insourcing dichotomy, the central role POSTAL plays in the European task force provides an interesting example of how insourcing can be complemented by the relationship management of external capabilities (including competitors). Although such an open approach might be difficult to apply to other organizations, such as ROYALPOL, given the nature of its operation, it is still interesting to note that our empirical data show a tension at ROYALPOL toward innovating its security management. There was concern that innovations would introduce new vulnerabilities. This concern is due to the endemic complexity of information security management that faces dynamic and sophisticated threats and hence may require an open approach for the development of dynamic capabilities. The concept of platform organizations [42] together with evidence from the open-source phenomenon [47] in public and private organizations helps frame this problem and informs the design of new organizational forms that implement a balanced strategy in practice.

The differences evidenced in the three cases are also reflected in the stability of the environment in which the organizations operate. This stability helps explain the different choices made by these organizations in both IT governance (i.e., outsourcing) and information security management. An in-depth investigation of the motivations for the outsourcing decisions of RAII, ROYALPOL, and POSTAL is outside the scope of the present paper. Nevertheless, our analysis confirms the necessity of a holistic analysis of bidirectional nonlinear relationships as opposed to a more traditional contingent view of outsourcing/insourcing decisions. Further research in this direction could extend the strategic dimension of information security related to the scope of the current configurational approach in the outsourcing literature [19].

Choosing the correct balance is certainly more complex than choosing between military and civilian strategies. There are implications from the abovementioned cases regarding incorrectly balanced strategies or a heavy inclination toward one paradigm or another. There would be predictable outcomes. If an organization existing in a highly volatile security situation over-focused on the prevention paradigm, the weaknesses in response preparedness are likely to lead to heavy losses in the event of an APT attack. In contrast, if an organization existing in a more stable situation over-focused on the response paradigm, the weaknesses in prevention are likely to lead to continual losses to well-known attacks. In either case, the losses would be accompanied by inefficiency in the use of security resources (overspending in the wrong areas and under-spending in the right areas). In the same vein, a strategy balancing the two paradigms (when a more singular focus on prevention or response may better suit the situation) would make security more expensive than due care would suggest.

8. Conclusion

The analysis of the three cases through the lens of the incident-centered framework provides insights on the balance between the prevention and the response approaches to information security management, as shown in Table 2. These insights are crystallized in the following propositions:

- Information security strategies employ principles and practices grounded in both the prevention and the response paradigm.
- Although the prevention paradigm may be dominant in contemporary commercial organizations, response paradigm principles and practices aimed at managing unpredictable threats (such as disaster recovery planning) retain an important role in protecting information security.
- Although the response paradigm may be dominant in military organizations, prevention paradigm principles and practices (such as firewalls and deterrent policies) retain an important role in protecting information security.

An incident-centered analysis of information security settings reveals an organization’s effective information security strategy and provides insights and understanding about how the organization chooses to balance between prevention and response paradigms as grounds for its current information security posture.

Future research is needed to investigate how these propositions lead to more detailed management principles based on the incident-centered framework. The centering of security management on the moment-of-incident should provide the most ideal use of security resources by erecting a comprehensive security architecture that ideally balances both prevention and response. With further work, this framework may lead to better risk management methods and an opportunity for the development of new information security risk management tools based on a more complete security strategic framework. For example, each of the three cases in our study appeared to have rationally balanced strategies, and each reported no major recent losses. It would be interesting to use this framework to analyze post hoc whether organizations that experienced major breaches adopted inappropriate balance strategies for their settings.

The information security manager of POSTAL represented the balance of the prediction and response paradigm in information security management strategies as follows:

“Information Security shouldn’t be thought as the security of a closed and barricaded castle, but as the security of an airport, crossed by millions of people, where the exact control of who enters and leaves is not possible, but however security of processes and smooth operations must be guaranteed, so that the whole machine has to work regardless of who enters and leaves. Nevertheless processes that recognize and block the anomalies must be activated. Response must be quick.”

Incident-centered information security management is a theoretical and practical framework consisting of three elements: (1) situational analysis, planning, and operation in the prevention paradigm; (2) situational analysis, planning, and operation in the response paradigm; and (3) close attention to the time continuum in deciding the balance of effort between (1) and (2).
The increasing sophistication in attacks suggests that many organizations may need to reconsider their balance between prevention and response strategies. While a dependence on the prevention paradigm works with repetitive and low-sophistication attacks, progressively more sophisticated attacks demand the increasing use of the response paradigm. Managers who understand the incident-centered model and whose environment reflects increasing sophistication in attacks will recognize the need to place additional emphasis on activities in the organization’s response paradigm.

Appendix A. Interview guide

1. What are the concerns and motives of the information security measures at your organization?
2. What is the focus of your organization’s information security management (prevention of future security attacks or quick response to security attacks)?
3. [Prevention/Response Paradigm] Depending upon the participant’s answer to Question #2.
   a. Do you think security risk is predictable or unpredictable? Why do you think so? What does your organization do to handle such risk?
   b. Do you think security risk is measurable or immeasurable? Why do you think so? What does your organization do to handle such risk?
   c. Do you think security risk is persistent or transient? Why do you think so? What does your organization do to handle such risk?
   d. As to the three types of risks we mentioned, do you think these characteristics change over time? If so, how do you think these characteristics change? What factors affect this change?
   e. How does your organization respond when security measures are compromised?
4. Do you think your organization’s information security focus changes over time, before/after the security incident? If so, please describe the changes.
   f. What changes occur?
   g. What factors made the changes?
   h. How do the changes occur?

References


Richard L. Baskerville is a Board of Advisors Professor of Information Systems (IS) at Georgia State University. His research regards security of IS, methods of IS design and development, and the interaction of IS and organizations. He is a Chartered Engineer and holds a Ph.D. from The London School of Economics, University of London. He is Editor Emeritus of the European Journal of Information Systems.

Paolo Spagnoletti is an Assistant Professor of Advanced Organization Design at LUISS Guido Carli University where he coordinates the Research Centre on Information Systems (CeRSI). He received his Ph.D. from LUISS and has been visiting fellow at LSE, Georgia State University and University of Agder. His research interests are on digital platforms, information infrastructures, and IS security. His works are published in Communications of AIS, International Journal of Accounting Information Systems, Journal of Theoretical and Applied E-Commerce Research, Journal of Information System Security and conference proceedings.

Jongwoo Kim is an Assistant Professor of Management Sciences and Information Systems (MSS) at the University of Massachusetts Boston. He received his Ph.D. degree in CIS from the Georgia State University. His work appears in IEEE Transactions on Engineering Management, IT and People, Software Process Improvement and Practice, International Journal of Intelligent Information Technologies, and several conferences. His research interests include IS Security, conceptual modeling, and IS in inter-organizational networks.