Information Security Strategies: Towards an Organizational Multi-Strategy Perspective

Atif Ahmad, Sean B. Maynard, Sangseo Park*

Department of Computing and Information Systems,
Melbourne School of Engineering,
The University of Melbourne,
Parkville, Victoria 3010, Australia.

* Contact Author: Sangseo Park
E-mail: parks@pgrad.unimelb.edu.au
Phone: +61 3 8344 1500
Fax: +61 3 93494596

Abstract

There considerable advice in both research and practice oriented literature on the topic of information security. Most of the discussion in literature focuses on how to prevent security attacks using technical countermeasures even though there are a number of other viable strategies such as deterrence, deception, detection and response. This paper reports on a qualitative study, conducted in Korea, to determine how organizations implement security strategies to protect their information systems. The findings reveal a deeply entrenched preventive mindset, driven by the desire to ensure availability of technology and services, and a comparative ignorance of exposure to business security risks. Whilst there was some evidence of usage of other strategies, they were also deployed in a preventive capacity. The paper presents a research agenda that calls for research on enterprise-wide multiple strategy deployment with a focus on how to combine, balance and optimize strategies.

Keywords: Information Security Strategy, Deterrence, Prevention, Compartmentalization, Deception, Defense in Depth

Introduction

Organizations are increasingly aware of the role that information and its associated technologies play in almost all organizational functions, especially in driving innovation and generating competitive advantage. In the modern information environment, organizational information and technology services are exposed to a range of security risks, including leakage of sensitive information and prolonged disruption to email and internet access, resulting in significant impact to business continuity. To address these security risks, an organization must implement an information security strategy through the establishment of a comprehensive framework to enable the development, institutionalization, assessment, and improvement of an information security program. In particular, the information security strategy must support the overall organization's strategic plans with its content clearly traceable to these higher-level sources (Bowen et al. 2006).

While organizations typically deploy 'baseline' security measures, the number of security incidents continues to increase. Literature evidence suggests that over 60% of organizations are employing technical information security countermeasures, including anti-virus software, firewalls, anti-spyware software, virtual private networks (VPN's), vulnerability/patch management, encryption of data in transit, and intrusion detection systems (Richardson 2011; Kessel 2011). However these reports also point out that organizations have experienced targeted attacks continuously and on an increasingly frequent basis. Further, these same studies show that security risk is increasing due to increased internal and external threats. Subsequently, security is getting harder to manage.

In this climate, organizations must employ strategies to direct their security efforts and should optimize their limited resources (Tirenin and Faatz 1999; Edwards and Willimas 2001; Saydjari 2004; Anderson and Choobineha 2008). However a single strategy may not be enough. Richards and Davis (2010) argue that organizations should utilize multiple information security strategies in order to ensure effectiveness of security measures and to maintain security policies.

A considerable amount of literature on the topic of information security exists, including best-practice standards and guidelines, and technical whitepapers on the implementation of information security controls (AS 270001, NIST Standards, etc). Various technical and, more recently, managerial information security issues are being subject to much scrutiny in both researcher and practitioner journals. Much of the literature discusses operational aspects of information security focusing on the topic of security controls and their deployment towards 'prevention' of security attacks on organizations. However, besides prevention, there are a number of security strategies conceptually identified in literature, such as: detection, deterrence, and deception (Tirenin and Faatz 1999). There has been little field-work conducted to determine which security strategies are employed by organizations to address the range of security risks, and how these strategies are deployed. Therefore, this paper poses the following exploratory research question *'How can organizations use security strategies to protect information systems?'*

This study conducted a comprehensive literature review across information security as well as in areas where security strategy is likely to be discussed, such as in military sources. Nine security strategies are identified. A qualitative focus group approach is used to determine how these security strategies are used in organizations. Security Managers from eight organizations were asked in the focus groups to discuss security strategies

employed in their organizations. The findings suggest that a large proportion of organizations use a preventive strategy to maintain availability of technology services. Some of the other identified strategies were used at an operational level to support the prevention strategy. Security managers largely ignored business security risks. In general, strategies were deployed in an ad-hoc manner without a formal and systematic approach to addressing risks through a combination of strategies.

Literature Review

Strategy is a concept that has evolved from a military setting where it is best described as: deciding what means to use, how to use it and how to apply it (Howard 1979). From a business perspective Beckman and Rosenfield (2008) define strategy as "deciding on where you want your business to go and figuring out how to get there". These definitions can be directly applied to information security strategy. Based on these perspectives (Park and Ruighaver 2008) define information security strategy as the "*art of deciding how to best utilize what appropriate defensive information security technologies and measures, and of deploying and applying them in a coordinated way to defense organization's information infrastructure(s) against internal and external threats by offering confidentiality, integrity and availability at the expense of least efforts and costs while to be effective"*.

Information security strategies have been defined and classified in a number of different ways and subsequently, there is no widespread agreement on their definition or classification. Studies have identified various strategies such as *Deterrence* (Straub and Welke 1998; D'Arcy et al. 2009), *Prevention* (McDermott 2000; Lampson 2004), *Surveillance* (Doyle et al. 2001; Dourish and Redmiles 2002), *Detection* (Henauer 2003; Stolfo 2004), *Response* (Beauregard 2001; Cahill 2003), *Deception* (Michael 2002; Carroll and Grosu 2009), *Perimeter Defense* (Snyder 2006), *Compartmentalization* (Tirenin and Faatz 1999) and *Layering* (Alberts 1996; Byrne 2006) which are each summarised in Table 1.

Table 1: Synthesis of Security Strategy areas in literature

Strategy	Definitions and literature
Prevention (PREV)	Prevention aims to protect information assets prior to an attack by prohibiting unauthorized access, modification, destruction, or disclosure. (Arce and McGraw 2004; Brand 1990; Browne 1972; Brykczynski and Small 2003; Evans et al. 2004; Graham 2003; Humphries et al. 2000; Lampson 2004; Lippmann et al. 2002; McDermott 2000; Ray et al. 2005; Schudel and Wood 2001; Virta 2005; Wood and Duggan 2000; Zalenski 2002)
Deterrence (DETER)	Deterrence employs disciplinary action to influence human behavior and attitude. (Agrell 1987; Blumstein et al. 1978; D'Arcy et al. 2009; Dunn 1982; Forcht 1994; Hu et al. 2011; Huth 1999; Kankanhalli et al. 2003; Klete 1975; Park et al. 2011; Parker 1981, 1983; Siponen and Vance 2010; Straub 1990; Straub and Nance 1990; Straub and Welke 1998; Waterman 2009)
Surveillance (SURV)	Surveillance is the systematic monitoring of the security environment towards developing situational awareness to assist in adapting to fast-changing circumstances and threats (Alberts 1996; Barford et al. 2010; Bearavolu et al. 2003; CSSP 2009; Debar et al. 2005; Dourish and Redmiles 2002; Doyle et al. 2001; Ohno et al. 2005; Roman et al. 2008)

Table 1: Synthesis of Security Strategy areas in literature	
Strategy	**Definitions and literature**
Detection (DETECT)	Detection is an operational-level strategy aimed at identifying specific security behavior (Debar and Tombini 2005; Eilertson et al. 2004; Hamill et al. 2005; Henauer 2003; Liu et al. 2001; Rytz et al. 2003; Shimeall et al. 2001; Stolfo 2004)
Response (RESP)	Response takes appropriate corrective actions against identified attacks. (Armstrong et al. 2004; Beauregard 2001; Cahill 2003; Hamill et al. 2005; Grance et al. 2004; Saydjari 2004; Williamson 2004)
Deception (DECEP)	Deception distracts an attacker's attention from critical information assets using decoys thereby leading the attacker to waste time and resources (Anderson 2001; Artail et al. 2006; Cao et al. 2004; Carroll and Grosu 2009; Chakrabarti and Manimaran 2002; Cohen 1998; Cohen and Koike 2004; Fowler and Nesbit 1995; George et al. 2004; Honeynet-Project 2001; Jaatun et al. 2007; Lakhani 2003; Michael 2002; Michael and Wingfield 2003; Ning and Xu 2003; Rice et al. 2011; Rowe 2003, 2006; Rowe et al. 2007; Ruiu 2006; Tinnel et al. 2002)
Perimeter Defense (PERI)	Perimeter defense creates a boundary around information assets that is secured by regulating traffic at every incoming and outgoing information channel (choke points). (Snyder 2006; McGuiness 2001; Shirey 2007)
Compartment-alization (COMP)	Compartmentalization reduces an attacker's opportunities by dividing the intended area of attack into zones that are secured separately (Anderson and Hearn 1996; Bauer 2001; Tirenin and Faatz 1999)
Layering (LAYER)	Layering uses multiple countermeasures that function independently but increases the effectiveness of the defense when working together thereby posing a series of challenges to the attacker. The defensive system is designed to be resilient by overlapping the series of countermeasures, whereby each countermeasure complements the next so that if one fails another will back it up. (Alberts 1996; Anderson 2001; Butler 2002; Byrne 2006; Dasgupta 2004; Gandotra et al. 2009; Hitchins 1995; Hunter 2003; Jones 2005; Kewley and Lowry 2001; Lester and Smith 2002; McGuiness 2001; McHugh et al. 2000; Peterson 2007; Price 2010; Rosenquist 2008; Rubel et al. 2005; Runnels 2002; Sharlun ; Smith 2002; Stytz 2004; Burnburg 2003)

From the literature review, two fundamental dimensions of strategies were identified: time and space. From a temporal (time) perspective, strategies can be deployed in anticipation of an attack or once an attack has been experienced. From a spatial (space) perspective, how the 'battlefield' space is designed plays a key role. For example breaking up the battlefield into zones to separate trusted and un-trusted computing systems can prevent an attack on an un-trusted computing system from penetrating trusted space. Finally, from a decision-making perspective, deciding on the specific tactics of attack and response also influences strategy. The following sections define and discuss strategies identified in literature.

Prevention (PREV)

Prevention aims to protect information assets prior to an attack by prohibiting unauthorized access, modification, destruction, or disclosure (Liu et al. 2001). Approaching information security strategy from a

purely preventive mindset implies that the organization has little tolerance for impact of any kind; therefore countermeasures must be deployed with a view to blocking all attacks on the organization.

Prevention strategies can be used to avoid information leakage. For example, a clean desk policy enforced by periodic inspections for misplaced and sensitive documents can be useful. From a technical point of view, barriers can be installed around valuable assets prior to an attack (Kankanhalli et al. 2003; Tirenin and Faatz 1999). A commonly used prevention control is authentication, which aims to limit access to authorized users (Brand 1990; Liu et al. 2001; Graham 2003; Lampson 2004). Further prevention techniques include the utilization of software that regulates user interaction with information assets (Browne 1972; Liu et al. 2001), encrypting information flowing over networks to prevent leakage - even if the network is compromised, using firewalls to filter network traffic, and using intrusion detection systems that employ anomaly and signature detection paradigms to identify suspicious data (Zalenski 2002; Liu et al. 2001).

The importance of scanning systems for vulnerabilities, and subsequently patching these vulnerabilities, has been recently highlighted (Humphries et al. 2000). As a result, updating and patching application systems has become a critical preventive technique aimed at denying attackers pathways into the organization. Additionally, vulnerability checking is being used to probe possible or potential weak points in the security infrastructure, aggressively using techniques named “red teaming” or “penetration testing” (McDermott 2000; Wood and Duggan 2000; Schudel and Wood 2001; Lippmann et al. 2002; Arce and McGraw 2004; Evans et al. 2004; Ray et al. 2005; Virta 2005).

Deterrence (DETER)

Deterrence employs disciplinary action to influence human behavior and attitude (Forcht 1994). When applied within organizations, the effectiveness of deterrence is influenced by two key factors – certainty of sanctions and severity of sanctions. The certainty of sanctions (i.e., the probability of being caught) is influenced by the level of awareness of the kind of sanctions, as well as the ability of enforcing bodies to detect offending behavior. The severity of sanctions is influenced by the range of sanctions that can be imposed (Blumstein et al. 1978; Straub 1990; Kankanhalli et al. 2003; Siponen and Vance 2010).

In the west, civilian organizations can only apply security strategies in a defensive capacity. Therefore, deterrence is typically applied internally, targeting company personnel. Deterrence is effective in guiding employees towards legitimate, acceptable use behavior (Klete 1975; Parker 1981, 1983), in discouraging weakly motivated internal perpetrators (Dunn 1982), in reducing insider abuse and misuse of information systems (Straub 1990; Straub and Nance 1990), and in influencing employee intentions (D’Arcy et al. 2009). The strategy is grounded in criminology and has been widely accepted in the military, international relations, and information warfare (Alberts 1996; Agrell 1987; Tirenin and Faatz 1999; Waterman 2009; Huth 1999).

One of the main foci of deterrence is in security policy, where deterrence has been used to specify punishment of employees that fail to adhere to policy statements. Straub and Welke (1998) emphasize that organizations should operate an education and training program to inform employees of organizational policy and guidelines in order to make information security efforts more effective. Additionally, Straub (1990) reports that deterrence efforts, such as the severity of penalties, awareness of deterrence actions, and the number of security staff have been successful in the reduction of computer abuse.

Others have found that deterrence efforts have a positive effect on information security, although the severity of penalties did not influence effectiveness (Kankanhalli et al. 2003). More recently, D'Arcy et al. (2009) found that the severity of penalty influenced the amount of abuse in a significant way, which is contrary to Kankanhalli et al. (2003)'s outcomes. Siponen and Vance (2010) recommended that organizations should increase training in security policy compliance and should focus on policing policy breaches. However, Hu et al. (2011) identified that deterrence using punishment alone was insufficient in enforcing information security and suggest that organizations reduce the perceived value of information assets. They also state that organizations need to employ high moral standards and self-control (Hu et al. 2011); in essence stating that security culture will influence deterrence efforts. This is in line with recent studies conducted in security culture (DaVeiga & Eloff 2010; Lim et al. 2012).

Surveillance (SURV)

Surveillance is the systematic monitoring of the security environment aimed at developing situational awareness to adapt to fast-changing circumstances and threats (Doyle et al. 2001). Situational awareness enables security decision makers to better cope with information security incidents and develop more effective defenses (Bearavolu et al. 2003).

Monitoring the information security environment of an organization in the physical and digital sphere using technical and non-technical means is challenging. Monitoring of various aspects of an individual's interaction with information and information systems includes logging access to restricted physical and logical spaces where hardcopy and softcopy information is kept.

From a technical point of view surveillance typically uses information generated from strategically placed 'sensors' augmented with visualization tools to increase security managers' understandability of the situation (Ohno et al. 2005; Doyle et al. 2001; CSSP 2009). Information collected for surveillance is typically sourced from systems and applications software (Dourish and Redmiles 2002), including intrusion detection systems that report on the number of attacks, degree of attack propagation, and type of attack (Ohno et al. 2005).

Detection (DETECT)

Detection is an operational-level strategy aimed at identifying specific security behavior (Hamill et al. 2005). The objective of detection is to allow the organization to react in a targeted manner. This strategy contrasts with surveillance in that the latter aims to understand the overall situation. Detection therefore, focuses on a specific event whereas surveillance observes the status as a whole.

Detection takes many forms including identification of malicious or unusual behavior (Eilertson et al. 2004), intrusion or misuse (Liu et al. 2001), and specific attacks against web servers (Debar and Tombini 2005). Additionally detection can be used to trigger the gathering of evidence of misuse regarding suspicious activity as well as identification of perpetrators (Straub and Welke 1998). Various security technologies are used within the detection strategy including dedicated computer and network intrusion detection devices, network scanners, system scanners, misuse and anomaly detectors, content screening and antivirus software, and audit programs (Liu et al. 2001; Tapiador & Clark 2011).

To be useful to an organization's security managers, detection of attacks and reporting must be timely and false alarms must be minimized (Hamill et al. 2005). Information provided to security managers stemming from detective measures should ideally be actionable and useful, such as whether an attack has begun, when the attack began, and the scope of the attack (Alberts 1996; Shimeall et al. 2001; Henauer 2003; Rytz et al. 2003; Stolfo 2004).

Response (RESP)

Response takes appropriate corrective actions against identified attacks. The response to an attack can be divided into two phases. Firstly the reaction phase, where appropriate actions are taken against the attacker/attack and secondly the recovery phase, where the situation is restored to its original state (Armstrong et al. 2004; Tirenin and Faatz 1999; Saydjari 2004; Hamill et al. 2005).

Security managers have considerable tactical options depending on how they want to react to an attack. For instance, a reaction may be to 'exclude' an attacker by transporting them to a different position (Lampson 2004). Response could be implemented by dropping a connection, blocking a suspicious IP address at a perimeter firewall or by employing a deception strategy by the use of a honeypot. Another tactic is containment, which separates the attacker and/or attacked area from other (unaffected) areas (Grance et al. 2004). Lastly, it is worth noting the literature also discusses offensive responses such as 'strike-back' (Welch et al. 1999) and 'strike-first' even though they are not legal options for private organizations in the Western World.

In the digital environment, an automated response is particularly important given the relative speed of attack compared to the speed of human decision-making (Williamson 2004). In this situation, a previously designated response to pre-defined conditions of threat, attack, and/or damage can be taken (Tirenin and Faatz 1999; Beauregard 2001; Cahill 2003).

Deception (DECEPT)

The Deception strategy distracts an attacker's attention from critical information assets using decoys, thereby, leading the attacker to waste time and resources (Cohen 1998; Tirenin and Faatz 1999). The concept of the Deception strategy originates in the military discipline where it is defined as the ability to "enhance, exaggerate, minimize, or distort capabilities and intentions; mask deficiencies; and otherwise cause desired appreciations where conventional military activities and security measures were unable to achieve the desired result" (JCS 1996, 1998). Deception has two constructs: passive deception and active deception. Passive deception focuses on hiding something, whereas active deception focuses on showing something (Rice et al. 2011). The techniques of the passive deception include concealment and camouflage; whilst in active deception include false and planted information, ruses, displays, demonstrations, feints and lies (Cohen 1998). According to Rice et al. (2011) and Fowler and Nesbit (1995) there are several principles of effective deception including: reinforcement of the adversary's expectations, realistic timing and duration, and coordination with the concealment of true intentions. These can also be applied in the information security domain.

In information security, deception is used to persuade an adversary to believe that false information they were given was actually true, thus driving them towards changing a course of action to what the defender intended, or to expose an attacker to other defensive measures (Tirenin and Faatz 1999; Rice et al. 2011). Deception has

proved effective in misdirecting attackers, even groups of skilled attackers, to a fake, imitation information system where they could be observed without endangering the organizations real systems (Cohen and Koike 2004). In order to guide an adversary to such a system, a decoy is used to grab the attention of attackers (Tinnel et al. 2002). Two types of decoys have been discussed - software decoys and honeypots. A software decoy is a wrapper that communicates with calling processes or threads on behalf of critical software (Michael 2002; Michael and Wingfield 2003). When using software decoys, attention may have to be paid regarding the technical misuse since the decoy is implemented with software which is intrinsically vulnerable and imperfect (Michael and Wingfield 2003). Honeypots are designed to trap unauthorized attackers by convincing them that the system is a real and valuable target to compromise (Honeynet-Project 2001; Rowe 2006; Carroll and Grosu 2009). A honeypot buys security manager's time while an attacker expends resources to compromise the honeypot (Chakrabarti and Manimaran 2002; Tirenin and Faatz 1999; Lakhani 2003; Ning and Xu 2003; Rowe 2003; Liu et al. 2005; Artail et al. 2006; Ruiu 2006).

Perimeter Defense (PERI)

A perimeter is a "physical or logical boundary that is defined for a domain or enclave and within which a particular security policy or security architecture applies" (Shirey 2007). In the context of information security, perimeter defense involves the creation of a boundary around information assets that is secured by regulating traffic at every incoming and outgoing information channel (choke points) (Schneier 2006, p109). Network firewalls, access control mechanisms, authentication mechanisms, countermeasures against (distributed) denial of service attacks are typical controls implemented as part of perimeter defense (Liu et al. 2001; McGuiness 2001).

According to Liu et al. (2001), perimeter defense can be useful for channel monitoring, prohibiting spyware installation, blocking reverse connections, and managing script kiddies. However, if it is the only line of defense then there is no secondary means of defense if it fails (McGuiness 2001). Snyder (2006) suggests that using a perimeter defense strategy may not be optimal as connecting wireless devices to many networks is not difficult, and may expose the organization to other attacks, from the inside. For instance, the CEO uses their computer at home and at the office, and by connecting to the network at the office they may inadvertently begin to propagate malware, via email. This in turn negates the perimeter.

Compartmentalization (COMP)

Compartmentalization reduces an attacker's opportunities by dividing the intended area of attack into zones that are secured separately (Schneier 2006, p105). In this way, an attacker that has overcome the defenses of one zone does not automatically have access to all other zones. Compartmentalization is frequently used in the military to secure information flows. Information is classified into categories such as secret and top-secret. Personnel are assigned clearances that dictate which category of information they can access. This technique can prevent individuals with access to the organization from accessing all information and makes it progressively more difficult to access information of higher classifications.

Compartmentalization can also be used to protect networks and computing systems. A typical example of this strategy is a DMZ (De-Militarized Zone) or a network area isolated from the internal network but open to public

to allow access from the outside the company (Bauer 2001). Publicly accessible 'proxy' servers (e.g. for web and database services) are located inside the DMZ to prevent external traffic from directly interacting with trusted internal servers.

Layering (LAYER)

Layering uses multiple countermeasures that function independently, but increases the overall effectiveness of the defense when working together, thereby posing a series of challenges to the attacker. The defensive system is designed to be resilient by overlapping a series of countermeasures, where each countermeasure complements the next, so that if one fails, another will back it up (Tirenin and Faatz 1999; Kewley and Lowry 2001; Alberts 1996; Smith 2002; Lester and Smith 2002; Stytz 2004; Jones 2005; Hitchins 1995; Rubel et al. 2005; Price 2010; Runnels 2002; Byrne 2006; Butler 2002; Burnburg 2003; Snyder 2006). The strategy originates from the design of medieval castles that featured concentric walls aimed at slowing down the progress of enemies whilst castle defenders engaged the enemy from towers (Price 2010; Hitchins 1995).

Layered defense is predicated on the belief that a single strategy is insufficient to handle the attacker's arsenal of sophisticated, intelligent, and innovative technologies (Kewley and Lowry 2001; Rosenquist 2008; Gandotra et al. 2009; Price 2010). Given the vulnerabilities in the intrinsically complex and imperfect software platforms in organizations, perfect security is impossible (Sharlun 2002; Lampson 2004; Price 2010). However, multiple defensive layers with different sets of vulnerabilities are more difficult to defeat than a single layer and create significant delay which benefits the defending side (Byrne 2006; Gandotra et al. 2009). Attackers consume their resources and time while they are trying to devise ways to overcome the hurdles on their attack path (Tirenin and Faatz 1999; Anderson 2001; Stytz 2004), attacks are mitigated and damage to the information assets is minimized (Peterson 2007; Sharlun 2002).

Several studies have shown layered defense to be effective in handling attacks against information assets. McHugh et al. (2000) found that layering increases security. Kewley and Lowry (2001) showed that layered defense is effective in mitigating attacks through three experiments mobilizing "red teams". Stytz (2004) posited that layered defense is cost-effective and more resilient than perimeter defense.

Summary

This section discussed nine strategies identified in literature as playing an important part in the management of organizational information security. Additionally it identified two dimensions where these strategies would be applied (temporally and spatially). The methodology and data collection is described in the following section followed by the evidence from the focus groups in the findings section.

Methodology and Data Collection

This study is the first phase of a large mixed methods project focusing on the use of security strategies in organizations. In this phase an empirical, qualitative research strategy was adopted since the research is exploratory. This took the form of two focus groups held in Korea. The next phases of the research will

conduct another round of focus groups, this time in Australia, and will perform a number of case studies with the ultimate goal of developing an architecture of security strategies.

To explore how security strategies are developed and utilized in organizations, a set of focus groups was conducted in this phase of the research with personnel responsible for the security management function. Whilst interviews or case studies could have been utilized for this study, (Kitzinger 1995) suggests that focus groups are better suited for the generation of ideas and often result in the discussion progressing in unexpected directions. Focus groups are ideal for this form of research as they allow the researcher to gain insight through the interaction of participants. Furthermore, using focus groups in this phase of the research is critical to enable the researchers to explore and to refine the research concepts at a deep level of understanding prior to engaging in other forms of data collection.

In this research, focus groups of up to 3 hours duration were conducted (see table 2) to examine how participants' organizations implemented security strategy. All participants in the focus groups had more than five years experience in information security management and were employed by medium to large organizations. Table 2 presents more detail about each participant, their job position, and the type of industry in which they work. The focus groups were conducted in Korean and were transcribed, then translated into English by the third named author.

Table 2: Focus Group participant details

Focus Group ID	**Participant Identifier***	**Position**	**Organization Area**
1	Kim	Security Manager	System integration
1	Cho	IT/security Manager	IT Solutions, services and consulting
1	Hong	Security Consultant	Security consulting
1	Lee	Security Manager	Software development
1	Choi	IT/security Manager	Manufacturing
2	Shin	Board Member/Security Consultant	Software development
2	Park	Security R&D Director	Software development
2	Han	Security R&D Manager	Software development
2	Kwon	Security Manager	Software development
2	Ki	Security Manager	System integration
2	Jung	IT Manager	System integration

*due to ethical considerations, pseudonyms are used for each participant

The focus group questions were open-ended and were designed to get participants to drive the discussion. The focus group discussion was structured in three main areas: 1) introduction of the session where group members got to know each other and the area of research was introduced, 2) the discussion – where participants were guided to discuss the various threats and the strategies used to mitigate those threats, and 3) the conclusions of

the session – where the researcher wrapped up the session. The researchers only interrupted to guide the conversation, but generally allowed participants to explore the various aspects around information security strategies.

The transcribed data was analyzed using a thematic content analysis (Krippendorff 1980; Miles and Huberman 1994) and drawing on the different categories outlined in Table 1 to classify collected evidence. In particular, the three authors assessed the evidence and discussed assessments collectively. In most instances, there was significant agreement between the authors on how the different mechanisms were classified. Additionally, a list of observations was developed for each focus group discussion pointing to subtle nuances or departures in the perspectives of the participants compared to the advice in literature. Findings in terms of the relevance of the different strategies used are presented in the section that follows.

Findings

This section presents the empirical findings from the focus groups. The findings draw on the structure of the different information security strategy areas listed in Table 1. Each area and associated set of mechanisms highlights (a) evidence from the field study that confirms the use of the strategy advocated in the research literature, (b) evidence where the participants mentioned that they operationalized the strategies differently compared to advice from the literature, and (c) strategies in literature, for which no empirical evidence were found in the cases. An overview of the findings is summarized in Tables 3 and 4.

Temporal Strategies

At an enterprise level all participants reported that their organizations used prevention as their first and primary strategy after which other strategies were considered. A range of technical and non-technical security measures were employed to prevent attacks from impacting organizations. Firewalls, intrusion detection systems and antivirus software were among the most common technical measures in place. From a non-technical perspective, participants reported the use of nondisclosure agreements and a code of conduct for employees for example. However, almost all of the participants reported that in their organization the measures were instituted as part of a preventive strategy even though they could be used for other purposes. This is confirmed by *Kim*, the security manager of a systems integration company. *"My company concentrates on preventive strategies very much. Most of our strategies and regulations are focused on prevention. Therefore, when we migrate services, we cease the services if there is any problem associated with prevention. On the other hand, relatively, the latter part [detection and reaction strategies] gets less attention. … Yes, prevention is substantially (the most important strategy of my company) …"* (*Kim*).

Some of the participants disclosed that their organization employed the deterrence strategy at a policy level by wording rules and procedures to create a fear of sanctions. However, there was one participant's organization that employed the deterrence strategy on employee behavior as well. *"My company checks if regulations are being complied with well or not on a periodic basis. Every identified violator is charged with a penalty for the violation"* (*Kim*). *Kim* went on to explain that the use of company information infrastructure was monitored through the use of software. Any detected violation of company security policy such as the use of unauthorized portable computing devices and USB drives resulted in punitive measures such as the withholding of employee

benefits and promotions. However, *Kim* pointed out that the strict regime of deterrence was not having the desired impact on employee behavior as the number of violations was not decreasing significantly and employees were inventing new ways of circumventing security controls.

The twin strategies of detection and response were used by the majority of participants' organizations to support the objective of preventing attacks. For example, the use of anti-virus software to detect and respond by eradicating or quarantining malware was systematically employed to prevent an attack from occurring. *"If a computer virus is detected, we block the port so that the virus can no longer be propagated … Even though it becomes problematic; we isolate the (infected) area so the virus does never spread all over the company"* (*Cho*). The same strategy was frequently directed towards email and network behavior. There was no evidence that detection was employed for learning purposes, such as part of a surveillance strategy towards gaining situational awareness.

There was no evidence from the participants that any of their workplaces employed deception tactics in any context. In fact, the security manager from one organization clearly stated that they were not interested in using deception strategies because they perceived the strategy would consume significant network bandwidth. *"From the viewpoint of normal organizations, deception is hard to employ. National institutions may use honeypots but it is very difficult for business organizations to use deception. It adds unnecessary cost for networks from the organizations' standpoint"* (*Hong*). The security managers, *Cho* and *Lee* also agreed that deception tactics were not feasible in their organizations. However, one of the other security managers thought deception was an excellent idea. Furthermore, whilst most participants' organizations did not use deterrence, it was discussed that there were organizations in Korea that actively used honeypots as part of a deception strategy directed at external attackers.

Table 3: Summary of Temporal Security Strategies observed in field study

Strategy	Security Strategy Defined	Evidence from field study
Prevention (PREV)	Prevention aims to protect information assets prior to an attack by prohibiting unauthorized access, modification, destruction, or disclosure.	*Evidence found in all organizations* Prevention is the primary strategy used by all organizations. A range of technical (e.g. software controls) and non-technical (e.g. Non-disclosure agreements) means were used to prevent information assets from being attacked or exploited.
Deterrence (DETER)	Deterrence employs disciplinary action to influence human behavior and attitude.	*Evidence found in some organizations* Confirmed in some cases at a policy level. Here the wording of policies is designed to influence the behavior and attitude of employees by instilling in them the fear of sanctions. In one case employee benefits/promotions were withheld as a means of punishment for violating security policies and procedures.

Table 3: Summary of Temporal Security Strategies observed in field study		
Strategy	**Security Strategy Defined**	**Evidence from field study**
Surveillance (SURV)	Surveillance is the systematic monitoring of the security environment towards developing situational awareness to assist in adapting to fast-changing circumstances and threats	*Evidence found in some organizations* There was no evidence of surveillance being used at an enterprise level however low-level monitoring was used in five organizations to detect security violations. No evidence of surveillance being used at an enterprise level however low-level monitoring was used in five organizations to detect security violations.
Detection (DETECT)	Detection is an operational-level strategy aimed at identifying specific security behavior	*Evidence found in some organizations* Used in five organizations to pinpoint the existence of viruses, to monitor email, detect malicious network behavior (using an Intrusion Detection System and general network monitoring)
Response (RESP)	Response takes appropriate corrective actions against identified attacks.	*Evidence found in some organizations* Organizations using detection to pinpoint attacks take actions in response. These responses were largely aimed at preventing the attack from occurring rather than learning about the security environment.
Deception (DECEP)	Deception distracts an attacker's attention from critical information assets using decoys thereby leading the attacker to waste time and resources	*No evidence found* No evidence of deception being used by any organization and the idea was controversial. Two participants clearly stated their opposition to the idea as they believed it would degrade network and systems performance. One participant thought it was a good idea.

Spatial Strategies

All organizations used a network perimeter to control information flow across organizational boundaries. At a minimum, the strategy incorporated a firewall that filtered network traffic, however there were other strategies frequently used such as network intrusion detection systems, spam mail filters, and Anti-DDoS (distributed denial of service) measures. *"It is normal to place an anti-DDoS device in front of a firewall in order. … An anti-spam gateway is also placed separately at the behind of a firewall"* (*Han*).

The majority of organizations prevented external users from gaining direct access to company servers by placing 'proxy' services (e.g. for web and database traffic) in zones (De-militarized Zone or DMZ). In addition to creating a DMZ, *Ki* stated that their organization also used *compartmentalization* to prevent unauthorized wireless devices from accessing the trusted internal network. *"We isolated an area, where unauthorized (mobile) terminal devices such as mobile phones or laptops can be connected to, from the rest of our (internal) area, where solely authorized devices are allowed to gain access."* (*Ki*). They went on to explain that the two zones were separated by a gate and that the physical act of passing through the gate would result in all portable wireless devices being switched from one zone to another.

There was no explicit evidence that organizations were using layering by design, even though some participants showed their interest in the strategic concept. Most organizations focused their temporal strategies and the majority of their security expenditure around their external perimeter firewall. Some participants stated that their organization employed intrusion detection systems and additional localized firewalls on systems and other internal subnets. In almost all cases there was an external firewall and internal countermeasures like anti-virus software, however there was no evidence that the multiple firewalls and other security measures were employed in combination as part of a high-level layering strategy.

Table 4: Summary of Spatial Security Strategies observed in field study

Strategy	Security Strategy Defined	Evidence from field study
Perimeter Defense (PERI)	Perimeter defense creates a boundary around information assets that is secured by regulating traffic at every incoming and outgoing information channel (choke points).	*Evidence found in all organizations* All organizations had a perimeter defense strategy in place. At a minimum the perimeter was enforced by a firewall.
Compart-ment-alization (COMP)	Compartmentalization reduces an attacker's opportunities by dividing the intended area of attack into zones that are secured separately	*Evidence found in some organizations* Compartmentalization manifested itself in the shape of a De-militarized Zone (DMZ) where proxy services were placed.
Layering (LAYER)	Layering uses multiple countermeasures that function independently but increases the effectiveness of the defense when working together thereby posing a series of challenges to the attacker. The defensive system is designed to be resilient by overlapping the series of countermeasures, whereby each countermeasure complements the next so that if one fails another will back it up.	*Evidence found in some organizations* At least two organizations had multiple security layers where a series of three firewalls were in place (internal, external, and systems). Almost all organizations had an external firewall and other countermeasures behind the firewall, like antivirus software however these were not considered 'layering' explicitly.

Discussion

There is considerable evidence to show that in all of the participants' organizations represented, security strategy is driven bottom-up rather than top-down. Firstly, the highest-ranking security role in the organization exists at a middle management level or lower. Secondly, although there were many references to industry standards and best-practice guidelines, security managers (with the exception of one participant) make no mention of driving strategy from organizational security policies or speaking to senior management on strategy-related issues. Discussing the resourcing of security strategy was the only time senior management were involved and the nature of the discussions strongly suggest that security managers did not have a permanent allocation in the budget for security expenditure which is further evidence that security is driven bottom-up.

Further, information security strategies are largely driven by technology availability considerations rather than strategic business objectives. Perhaps the best example is the way security managers address the protection of information assets. Given every organization retains information assets of varying levels of sensitivity (e.g. intellectual property and competitive advantage assets, client confidential information, internal private information such as payroll and salary information) it was surprising that all of the participants assumed organizational information to be a single asset requiring a single approach towards protection. The only security measures directed towards confidential documents and sensitive (explicit) knowledge was the wholesale encryption of hard disks to prevent corporate data from being read in case of leakage and high-level policy statements and non-disclosure agreements. There was no evidence that security managers were even aware of what kinds of sensitive information and knowledge existed, where they were stored, who had access to them and how the information was circulating in the organization. There was no evidence of sensitivity classification of information and handling procedures. Further, there were no strategies designed to limit information flows through compartmentalization.

Interestingly, there was little mention of formal security risk assessments when developing strategy. This is somewhat curious as participants frequently referred to best practice industry standards as a source of guidance and the majority of such standards clearly state security strategy must be driven by consideration of risk. Other security management functions that contribute to strategy were also not mentioned. For example, incident response and disaster recovery, security awareness and training, and other such functions were not mentioned by participants as having input into the development of security strategy.

Responsibility for security strategy in almost all cases lay with the technology part of the organization rather than the business side. Security managers typically had a technology background and techno-centric view of the world. Their attitude and belief is evident from their consistent focus on addressing every security threat with a technical countermeasure and reluctance to address the human dimensions through security awareness, training, education or by changing organizational culture towards security.

Organizations approach strategy with a preventive mindset driven by the need to ensure availability of technology and services rather than to preserve the confidentiality and integrity of information assets. That means the strategies designated as ‘preventive’ are the focus of their efforts but other strategies such as detection and response, and deterrence are also deployed from a preventive mindset. This leads to a rather futile situation with business security risks such as information and knowledge leakage. A techno-centric and preventive point of view creates a narrow focus on leakage through technologies and ignores conversations and movement of paper. Further, there is a strong motivation to take control of all technology and declare what cannot be controlled to be unsanctioned (like smartphones). Unfortunately, this focus ignores the need to influence the use of information and technology through human-centered initiatives such as the development of a security culture, education, training and awareness. The lack of focus on the latter has resulted in employees seeing controls as an inconvenience or challenge that must be circumvented thereby creating a sense of frustration for security managers such as in the case of *Kim’s* Company where the manager admitted that his deterrence strategy was not working as employees were circumventing controls.

This study exposed a lack of knowledge and an ad-hoc approach to security strategy in the sample of security managers. The evidence strongly implies that the security managers had little skill and no experience in

combining multiple security strategies to address the range of risks the organizations were exposed to. However, it must be said that the security managers were constrained in their ability to develop a viable security strategy. Senior management saw their role as purely technical, devoted to maintaining the availability of technology systems. The wholesale absence of the security risk assessment data and a formal and historical record of incidents indicated strategies were not being informed by relevant (and good quality) security data. As a result, security situational awareness was poor and strategies were narrowly focused with no clear avenues of feedback on their effectiveness.

Constraints on cost were an underlying theme of the discussions. Security managers felt they needed better tools to detect security violations which were considered too costly by senior management. Interestingly, in Korea the cost of labor in the middle and lower management is significantly cheaper than the West making it more palatable for senior management to create new security management roles rather than invest in expensive technical solutions. The relatively cheaper cost of labor could be seen as an opportunity to invest in developing a security analysis capability, unfortunately though the organizational focus on technical solutions prevents growth in this area.

An Agenda for Security Strategy Research in Information Systems

There are a number of observations from this study that influence future research directions in security strategy. Firstly, there has been little research approaching security strategy from a holistic and enterprise-wide perspective. The majority of literature discusses security strategy from a technical perspective without considering how the business perspective can be integrated. This is not surprising as research in the area of information security management has evolved out of the traditional area of information security which has been synonymous with IT security. Research in the area of information security management has recently begun to address the issues of governance, culture, risk and policy but there is little research in the area of enterprise security strategy.

Secondly, research on process lifecycles that guide security managers on how to address security risk effectively using high-level security strategies and a range of controls is needed (including how controls can be used in a variety of contexts to support multiple strategies). Significantly, research is needed on combining, balancing and optimizing strategies to address insider versus outsider threats and business versus technical security risks in various organizational security environments.

Thirdly, the impact of the complexity of the modern information environment on strategy selection is another key challenge for researchers. Many organizations operate in large-scale network environments with numerous servers, fixed terminals and portable wireless devices including laptops and smartphones. In addition, there are employees with complex access profiles to masses of information at varying levels of sensitivity. Devising strategies to contend with risk exposure in these security environments requires a systematic and comprehensive approach with a view to learning and developing situational awareness especially from security incidents. Research is needed in addressing complexity using learning and feedback strategies.

Finally, while there are many types of defensive strategies discussed in literature (Straub and Welke 1998; Lampson 2004; Doyle et al. 2001; Henauer 2003; Beauregard 2001; Michael 2002; Snyder 2006; Tirenin and Faatz 1999; Alberts 1996), such as prevention, detection, deterrence and deception etc., there is actually little research on how these different types of strategies can be applied in an organizational context.

Future Work and Limitations

There are a number of limitations to this study. The study was conducted in Korea within Korean organizations. Subsequently, there may be an issue of generalizability to organizations in other countries. In particular, the relative cost of technology to labor varies and therefore influences patterns of expenditure in security. However, there is a strong likelihood that the attitudes and beliefs of security managers regarding security strategy will be similar across countries. The study included a small number of organizations from similar industries with what appears to be similar risk profiles. Organizations that appoint security managers at a middle or lower management levels are likely to employ personnel with similar backgrounds to those in the organizations in this study. This is because a large number of security managers have an IT rather than business background. It can be argued that organizations with a high awareness of the sensitivity of their knowledge assets may approach security strategy differently however no such indications were found in the literature review.

In the second phase of this research project, another round of focus groups will be held with security managers in Australia. Security managers from organizations with strong business risk awareness and mature security management functions such as risk and incident response will be invited. The focus in this new context will be to examine the extent to how various security strategies are deployed, combined and optimized in response to the security environment.

Additionally, the final phase of the project will use in-depth case studies to investigate the relationship that organizations form between the different strategies identified in this paper. The overall aim of this phase is to develop an architecture of security strategies that will enable organizations to address the challenges of technological complexity and both business and technical risks in the modern security environment.

Conclusion

This paper reports on security strategies used in organizations. The findings show that most organizations see the problem of information security as one of availability of their information infrastructure. Hence, they focus their security efforts towards preventing attacks and use other strategies such as deterrence, and detection and response for preventive purposes.

This paper makes four key contributions. Firstly, information security strategies discussed in literature were identified and defined and categorized in terms of time and space. These strategies and the classification can be useful for future research. Secondly, the study highlighted a series of issues with the security strategy function in organizations. In particular, regarding senior management, the perceived limited role of security strategy, the lack of commitment to the security strategy function, and the low-level of involvement in strategizing hinders the development of security strategy within organizations. Thirdly, in terms of security management the focus

on technology risks to the exclusion of business risks, the low quality of risk related information and inability to effectively implement and combine security strategies were all identified.

Finally, the paper highlights a number of implications for future research. These include the need for research on a holistic approach to security strategy, which addresses business and technology risk and particularly guidance on how to combine and implement various strategies effectively.

References

Agrell W (1987) Offensive versus Defensive: Military Strategy and Alternative Defence. Journal of Peace Research 24 (1):75-85

Alberts DS (1996) Defensive Information Warfare. NDU Press Book, National Defense University,

Anderson EE, Choobineha J (2008) Enterprise information security strategies. Computers & Security 27:22–29

Anderson P (2001) Deception: A Healthy Part of Any Defense in-Depth Strategy. SANS Institute InfoSec Reading Room, February 15, 2001 edn. SANS Institute,

Anderson RH, Hearn AC (1996) An Exploration of Cyberspace Security R&D Investment Strategies for DARPA: 'The Day After ... in Cyberspace'. RAND,

Arce I, McGraw G (2004) Why Attacking Systems Is a Good Idea. IEEE Security & Privacy 2 (4):17-19

Armstrong D, Carter S, Frazier G, Frazier T (2004) Autonomic Defense: Thwarting Automated Attacks via Real-Time Feedback Control. Complexity 9 (2):41-48

Artail H, Safa H, Sraj M, Kuwatly I, Al-Masri Z (2006) A Hybrid Honeypot Framework for Improving Intrusion Detection Systems in Protecting Organizational Networks. Computers & Security 25:274-288

Barford P, Dacier M, Dietterich TG, Fredrikson M, Giffin J, Jajodia S, Jha S, Li J, Liu P, Ning P, Ou X, Song D, Strater L, Swarup V, Tadda G, Wang C, Yen J (2010) Cyber SA: Situational Awareness for Cyber Defense. Cyber Situational Awareness, Advances in Information Security (46):3-13

Bauer M (2001) Designing and Using DMZ Networks to Protect Internet Servers. Linux Journal 2001 (83)

Bearavolu R, Lakkaraju K, Yurcik W, Raje H (2003) A Visualization Tool for Situational Awareness of Tactical and Strategic Security Events on Large and Complex Computer Networks. Paper presented at the Military Communications Conference (MILCOM) 2003, 13-6 Oct.

Beauregard JE (2001) Modeling Information Assurance. Master's Thesis, Air Force Institute of Technology, Air University, Ohio

Beckman SL, Rosenfield DB (2008) Operations Strategy: Competing in the 21st Century. McGraw-Hill/Irwin, New York

Blumstein A, Cohen J, Nagin D (1978) Deterrence and Incapacitation: Estimating the Effects of Criminal Sanctions on Crime Rates. National Academy of Science, Washington, D.C.

Bowen P, Hash J, Wilson M, Bartol N, Jamaldinian G (2006) Information Security Handbook: A Guide for Managers. . NIST Special Publication 800-100. NIST, Gaithersburg, MD

Brand RL (1990) Coping with the Threat of Computer Security Incidents: A Primer from Prevention through Recovery, CERT, Pittsburgh, Pa., June 1990.

Browne PS (1972) Computer Security: A Survey. ACM SIGMIS Database 4 (3):1-12

Brykczynski B, Small RA (2003) Reducing Internet-Based Intrusions: Effective Security Patch Management. IEEE Software:50-57

Burnburg MK (2003) A Proposed Framework for Business Information Security Based on the Concept of Defense-in-Depth. Master's Thesis, University of Illinois at Springfield, Springfield, Illinois

Butler SA (2002) Security Attribute Evaluation Method: A Cost-Benefit Approach. Paper presented at the 24th International Conference on Software Engineering (ICSE '02), New York, NY,

Byrne P (2006) Application Firewalls in a Defence-in-Depth Design. Network Security (9):9-11

Cahill TP (2003) Cyber Warfare Peacekeeping. Paper presented at the 2003 IEEE Workshop on Information Assurance, Jun.

Cao J, Lin M, Deokar A, Burgoon JK, Crews JM, Adkins M (2004) Computer-Based Training for Deception Detection: What Users Want? ISI 2004, LNCS 3073:163–175

Carroll TE, Grosu D (2009) A Game Theoretic Investigation of Deception in Network Security. Paper presented at the 18th International Conference on Computer Communications and Networks (ICCCN '09), Jan

Chakrabarti A, Manimaran G (2002) Internet Infrastructure Security: A Taxonomy. IEEE Network 16 (6):13-21

Cohen F (1998) A note on the role of deception in information protection. Computers and Security 17 (6):483-506

Cohen F, Koike D (2004) Misleading attackers with deception. Paper presented at the Information Assurance Workshop, 2004. Proceedings from the Fifth Annual IEEE SMC, 10-11 June 2004

CSSP (2009) Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies. Control Systems Security Program, National Cyber Security Division, Department of Homeland Security,

D'Arcy J, Hovav A, Galletta DF (2009) User Awareness of Security Countermeasures and its Impact on Information Systems Misuse: A Deterrence Approach. Information Systems Research 20 (1):79-98

Da Veiga A & Eloff JHP (2010) A framework and assessment instrument for information security culture, Computers and Security 29(2):196-207.

Dasgupta D (2004) Immuno-Inspired Autonomic System for Cyber Defense. Computer Science Technical Report. Univ. of Memphis,

Debar H, Morin B, Boissee V, Guerin D (2005) An Infrastructure for Distributed Event Acquisition. Paper presented at the European Institute for Computer Antivirus Research(EICAR) 2005 Conference Best Paper, Saint Julians, Malta, Apr.

Debar H, Tombini E (2005) Accurate Detection of HTTP Attack Traces in Web Server Logs. Paper presented at the European Institute for Computer Antivirus Research(EICAR) 2005 Conf. Best Paper, Saint Julians, Malta, Apr.

Dourish P, Redmiles D (2002) An Approach to Usable Security Based on Event Monitoring and Visualization. Paper presented at the 2002 Workshop on New Security Paradigms, Virginia Beach, Virginia, USA, Sep.

Doyle J, Kohane I, Long W, Shrobe H, Szolovits P (2001) Agile Monitoring for Cyber Defense. Paper presented at the 2001 DARPA Information Survivability Conference & Exposition II (DISCEX '01), Jun.

Dunn TS (1982) Methodology for the Optimization of Resources in the Detection of Computer Fraud. University of Arizona,

Edwards S, Willimas MC (2001) The Need for In-Depth Cyber Defence Progrmmes in Business Information Warfare Environments. Paper presented at the 2nd Australian Information Warfare and Security Conf. 2001,

Eilertson EE, Ertoz L, Kumar V (2004) MINDS: A New Approach to the Information Security Process. Paper presented at the 24th Army Science Conference, Dec.

Evans S, Kyle DH, Piorkowski J, Wallner J (2004) Risk-Based Systems Security Engineering: Stopping Attacks with Intention. IEEE Security & Privacy 2 (6):59-62

Forcht KA (1994) Computer Security Management. Boyd and Fraser, Danvers, MA

Fowler C, Nesbit R (1995) Tactical deception in air-land warfare. Journal of Electronic Defense 18 (6):37-79

Gandotra V, Singhal A, Bedi P (2009) Threat Mitigation, Monitoring and Management Plan - A New Approach in Risk Management. Paper presented at the 2009 International Conference on Advances in Recent Technologies in Communication and Computing,

George JF, Biros DP, Adkins M (2004) Testing Various Modes of Computer-Based Training for Deception Detection. Paper presented at the ISI 2004, LNCS 3073,

Graham D (2003) It's All About Authentication. SANS Institute,

Grance T, Kent K, Kim B (2004) Computer Security Incident Handling Guide (trans: Computer Security Division ITL). NIST Special Publication. National Institute of Standards and Technology, Gaithersburg, MD

Hamill JT, Deckro RF, Kloeber-Jr. JM (2005) Evaluating Information Assurance Strategies. Decision Support Systems 39:463-484

Henauer M (2003) Early Warning and Information Sharing. Paper presented at the Workshop on Cyber Security & Contingency Planning: Threats and Infrastructure Protection, Zurich, Switzerland, Sep.

Hitchins DK (1995) Secure Systems-Defence in Depth. Paper presented at the European Convention on Security and Detection, 16-18 May

Honeynet-Project (2001) Know Your Enemy II: Tracking the Blackhat's Moves. The Honeynet Project,

Howard M (1979) The Forgotten Dimensions of Strategy. Foreign Affairs 57 (5):975-986

Hu Q, Xu Z, Dinev T, Ling H (2011) Does Deterrence Work in Reducing Information Securiuty Policy Abuse by Employees? Communications of the ACM 54 (6):54-60

Humphries JW, Carver-Jr. CA, Pooch UW (2000) Secure Mobile Agents for Network Vulnerability Scanning. Paper presented at the 2000 IEEE Workshop on Information Assurance and Security, United States Military Academy, West Point, NY, 6-7 Jun.

Hunter P (2003) Defence in Depth - Protecting the Queen. Network Security (6):17-18

Huth PK (1999) Deterrence and International Conflict: Empirical Findings and Theoretical Debate. Annual Review of Political Science 2:25-48

Jaatun MG, Nyre AA, Sørensen JT (2007) Survival by Deception. Paper presented at the SAFECOMP 2007, LNCS 4680,

JCS (1996) Joint Publication 3-58: Joint Doctrine for Military Deception.

JCS (1998) Joint Publication 3-13: Joint Doctrine for Information Operations.

Jones B (2005) Overview of DoD Defense in Depth Strategy. Global Information Assurance Certification Paper, 4 January edn. SANS Institute,

Kankanhalli A, Teo H-H, Tan BCY, Wei K-K (2003) An Integrative Study of Information Systems Security Effectiveness. International Journal of Information Management 23:139-154

Kessel Pv (2011) Into the Cloud, Out of the Fog: Ernst & Young's 2011 Global Information Security Survey

Kewley DL, Lowry J (2001) Observations on the Effects of Defense in Depth on Adversary Behavior in Cyber Warfare. Paper presented at the 2001 Workshop on Information Assurance and Security, U.S. Military Academy, West Point, NY, 5-6 Jun.

Kitzinger J (1995) Qualitative research: Introducing focus groups. British Medical Journal 311:299-302

Klete H (ed) (1975) Some Minimum Requirements for Legal Sanctioning Systems with Special Emphasis on Detection. Deterrence and Incapacitation: Estimating the Effects of Criminal Sanctions on Crime Rates. National Academy of Sciences, Washington, D.C.

Lakhani AD (2003) Deception Techniques Using Honeypots. MSc, University of London, UK,

Lampson BW (2004) Computer Security in the Real World. Computer 37 (6):37-46

Lester AJ, Smith CL (2002) An Investigation Into the Application of Defence in Depth Theory to Electronic Information Protection. Paper presented at the 3rd Australian Information Warfare and Security Conference 2002,

Lim JS, Chang S, Ahmad A, Maynard SB (2012) Towards A Cultural Framework for Information Security Practices. In: Gupta M, Walp J, Sharman R (eds) Strategic and Practical Approaches for Information Security Governance: Technologies and Applied Solutions. IGI Global,

Lippmann R, Ingols K, Scott C, Piwowarski K, Kratkiewicz K, Artz M, Cunningham R (2006) Validating and Restoring Defense in Depth Using Attack Graphs. Paper presented at the Military Communications Conference (MILCOM) 2006, Washington, D.C.,

Lippmann R, Webster S, Stetson D (2002) The Effect of Identifying Vulnerabilities and Patching Software on the Utility of Network Intrusion Detection. Paper presented at the 5th International Symposium on Recent Advances in Intrusion Detection(RAID), Oct.

Liu P, Zang W, Yu M (2005) Incentive-Based Modeling and Inference of Attacker Intent, Objectives, and Strategies. ACM Transactions on Information and System Security 8 (1):78-118

Liu S, Sullivan J, Ormaner J (2001) A Practical Approach to Enterprise IT Security. IEEE IT Professional 3 (5):35-42

McDermott JP (2000) Attack Net Penetration Testing. Paper presented at the 2000 Workshop on New Security Paradigms, Ballycotton, County Cork, Ireland,

McGuiness T (2001) Defense In Depth. SANS Institute InfoSec Reading Room. SANS Institute,

McHugh J, Christie A, Allen J (2000) Defending Yourself: The Role of Intrusion Detection Systems. IEEE Software 17 (5):42-51

Michael JB (2002) On the Response Policy of Software Decoys: Conducting Software-based Deception in the Cyber Battlespace. Paper presented at the 26th Annual International Computer Software and Applications Conf. (COMPSAC'02), Aug.

Michael JB, Wingfield TC (2003) Lawful Cyber Decoy Policy. Paper presented at the IFIP 18th Int'l Information Security Conf., May

Ning P, Xu D (2003) Learning Attack Strategies from Intrusion Alerts. Paper presented at the ACM CCS?3, Washington, D.C., USA., Oct.

Ohno K, Kike HK, Koizumi K (2005) IPMatrix: An Effective Visualization Framework for Cyber Threat Monitoring. Paper presented at the Ninth Int'l Conf. on Information Visualisation (IV?5), London, England,

Park S, Ruighaver AB, Maynard SB, Ahmad A (2011) Towards Understanding Deterrence: Information Security Managers' Perspective. Paper presented at the International Conference on IT Convergence and Security 2011, Suwon, Korea,

Park S, Ruighaver T (2008) Strategic Approach to Information Security in Organizations. Paper presented at the 2008 IEEE International Conference on Informarion Science and Security (ICISS 2008), Seoul, Korea.,

Parker DB (1981) Computer Security Management. Reston Publishing, Reston, VA

Parker DB (1983) Fighting Computer Crime. Scribner, New York

Peterson G (2007) Security Architecture Blueprint. Arctec Group, LLC,

Price SM (2010) A Defense-in-Depth Security Architecture Strategy Inspired by Antiquity. ISSA Journal 10-16

Ray HT, Raghunath, Kantubhukta HR (2005) Toward an Automated Attack Model for Red Teams. IEEE Security & Privacy 3 (4):18-25

Rice M, Guernsey D, Shenoi S (2011) Using Deception to Shield Cyberspace Sensors. Paper presented at the Critical Infrastructure Protection V, IFIP AICT, 3–18

Richards K, Davis B (2010) Computer Security Incidents Agaist Australian Businesses: Predictors of Victimisation. Trends & Issues in Crime and Criminal Justice (399):1-6

Richardson R (2011) 2010/2011 CSI Computer Security Crime & Security Survey. Computer Security Institute,

Roman R, Lopez J, Gritzalis S (2008) Situation awareness mechanisms for wireless sensor networks IEEE Communications Magazine 46 (4):102-107

Rosenquist M (2008) Defense in Depth Strategy Optimizes Security. Intel Information Technology,

Rowe NC (2003) Counterplaning Deceptions To Foil Cyber-Attack Plans. Paper presented at the 2003 IEEE Workshop on Information Assurance, Jun.

Rowe NC (2006) Measuring the Effectiveness of Honeypot Counter-Counterdeception. Paper presented at the System Sciences, 2006. HICSS '06. Proceedings of the 39th Annual Hawaii International Conference on, 04-07 Jan. 2006

Rowe NC, Custy EJ, Duong BT (2007) Defending Cyberspace with Fake Honeypots. JOURNAL OF COMPUTERS, 2 (2):22-36

Rubel P, Ihde M, Harp S, Payne C (2005) Generating Policies for Defense in Depth. Paper presented at the 21st Annual Computer Security Applications Conference, December

Ruiu D (2006) Learning from Information Security History. IEEE Security & Privacy 4 (1):77-79

Runnels MG (2002) Implementing Defense in Depth at the University Level. SANS Institute InfoSec Reading Room. SANS Institute,

Rytz R, Romer J, Henauer M (2003) MELANI- An Analysis Centre for the Protection of Critical Infrastructure in the Information Age. Paper presented at the Workshop on Cyber Security & Contingency Planning: Threats and Infrastructure Protection, Zurich, Switzerland, Sep.

Saydjari OS (2004) Cyber Defense: Art to Science. Communications of the ACM 47 (3):53-57

Schneier B (2006) Beyond Fear. Springer, New York, NY, USA

Schudel G, Wood B (2001) Adversary Work Factor as a Metric for Information Assurance. Paper presented at the 2001 Workshop on New Security Paradigms, Feb.

Sharlun G (2002) Defense in Depth: The lessons from Troy and the Maginot line applied. Global Information Assurance Certification Paper. SANS Institute,

Shimeall T, Williams P, Dunlevy C (2001) Countering Cyber War. NATO Review:16-18

Shirey R (2007) Internet Security Glossary, Version 2, Request for Comments: 4949. Network Working Group, IETF,

Siponen M, Vance A (2010) Neutralization: New Insights into the Problem of Employee Information Systems security Policy Vilations. MIS Quarterly 34 (3):487-502

Smith CL (2002) A Method for Understanding Students' Perceptions of Concepts in the Defence in Depth Strategy. Paper presented at the 3rd Australian Information Warfare and Security Conference 2002, Perth, WA,

Snyder J (2006) Six Strategies for Defense-in-Depth: Securing the Network from the Inside Out. Joel Snyder's Blog, vol 2011.

Stolfo SJ (2004) Worm and Attack Early Warning: Piercing Stealthy Reconnaissance. IEEE Security & Privacy 2 (3):73-75

Straub DW (1990) Effective IS Security: An Empirical Study. Information Systems Research 1 (3):255-276

Straub DW, Nance WD (1990) Discovering and Disciplining Computer Abuse in Organizations: A Field Study. MIS Quarterly 14 (1):45-62

Straub DW, Welke RJ (1998) Coping with Systems Risk: Security Planning Models for Management Decision Making. MIS Quarterly 22 (4):441-469

Stytz MR (2004) Considering Defense in Depth for Software Applications. IEEE Security & Privacy 2 (1):72-75

Tapiador JE & Clark JA (2011) Masquerade mimicry attack detection: A randomised approach, Computers and Security 30(5):297-310.

Tinnel LS, Saydjari OS, Farrell D (2002) Cyberwar Strategy and Tactics. Paper presented at the 2002 IEEE Workshop on Information Assurance, United States Military Academy, West Point, NY, Jun.

Tirenin W, Faatz D (1999) A Concept for Strategic Cyber Defense. Paper presented at the Military Communications Conference (MILCOM) '99,

Virta V (2005) The Red Team Toolbox, A Method for Penetration Tests. Paper presented at the European Institute for Computer Antivirus Research(EICAR) 2005 Conf. Best Pape, Saint Julians, Malta, Apr.

Waterman S (2009) U.S. Takes Aim at Cyberwarfare. The Washington Times, July 2,

Welch DJ, Buchheit N, Ruocco A (1999) Strike Back: Offensive Actions in Information Warfare. Paper presented at the 1999 Workshop on New Security Paradigms, Caledon Hills, Ontario, Canada, Sep.

Williamson MM (2004) Resilient Infrastructure for Network Security. Complexity 9 (2):34-40

Wood BJ, Duggan RA (2000) Red Teaming of Advanced Information Assurance Concepts. Paper presented at the DARPA Information Survivability Conference and Exposition, 2000. DISCEX '00, Hilton Head, SC, USA, 25-27 Jan.

Zalenski R (2002) Firewall technologies. IEEE Potentials 21 (1):24-29