Communications of the IIMA

Volume 9 | Issue 4 Article 2

2009

A Framework for Enterprise Security Architecture and Its Application in Information Security Incident Management

Yi-Ting Shen
California State University San Bernardino

Frank Lin
California State University San Bernardino

C.E. Tapie Rohm
California State University San Bernardino

A Framework for Enterprise Security Architecture and Its Application in Information Security Incident Management

Yi-Ting Shen
California State University San Bernardino
USA
sheny@csusb.edu

Frank Lin
California State University San Bernardino
USA
flin@csusb.edu

C.E. Tapie Rohm Jr.
California State University San Bernardino
USA
trohm@csusb.edu

ABSTRACT

An enterprise architecture (EA) plan is a long-term view or blueprint for an organization. It is a very important blueprint for balancing business and Information Technology (IT) and for adding value to an organization. Security is also nowadays an essential dimension for enterprises. It can prevent confidential information from being leaked, and/or stolen, lost succumbing to other serious disasters. There are many studies focusing on EA or on specific aspects of security. However, there are very few studies focusing on enterprise security architecture. This paper focuses on integrating the security dimension into the Zachman EA framework (Zachman, 2007) and is intended to serve as an enterprise security framework (ESA) to assist an organization in successfully and effectively implementing security. The efficacy of the ESA implementation is illustrated through an application in an organization.

INTRODUCTION

Security architecture is a concept that aims to design an infrastructure of information systems to ensure that they provide enough security to organizations and businesses (Sherwood, 2005). Today, most businesses rely on IT much more heavily than in the past. Carelessly designed security architecture has serious implications for a business, such as the high risk of being unable to do daily business operations. This heavy reliance on information systems highlights the importance of developing an efficient and effective security architecture within the entire enterprise.

Unfortunately, emphasizing security technology alone is not enough to produce effective and efficient security for an entire organization (Sherwood, 2005). Security technology itself is designed to resolve security issues without considering other factors, such as cost and business operating models. Businesses differ in terms of organizational scopes, sizes, capital capacities, business operating models, and top management support (Boh & Yellin, 2006). These factors

affect the security needs and the security trust level (Sherwood, 2005). This study proposes to use the Zachman framework as a basis for developing an enterprise security architecture. With such a framework, developers can clearly understand the security needs of businesses and the priority of implementing security projects in a specific time period and in a specific manner. In addition, with a plan based on this framework, developers have a very clear view of the entire procedure and are able to fully control the situation, such as the status of implementing these security needs, the impact, the ability to effectively respond to unexpected events and so on. Furthermore, an enterprise security architecture based on the Zachman framework allows developers to plan and examine new advanced information technology and systems with appropriate security solutions at once. This can not only provide new business opportunities by increasing the convenience and speed of business processes (Fumy & Sauerbrey, 2006), but can also guarantee the confidentiality, integrity, and availability of business information (Fumy & Sauerbrey, 2006). From the organizational perspective, it saves money. All of these advantages show that an enterprise security architecture based on the Zachman framework can produce effective and efficient security for an entire organization.

Section 2 discusses an enterprise security architecture based on Zachman's EA framework. A case study of an educational institution's information incident management report system is used to illustrate the efficacy of the developed framework which will be discussed in section 3. The result of this research is a guideline for an organization to efficiently create an enterprise architecture plan and to easily use this plan for transferring business security needs into IT security infrastructure and implementation.

FRAMEWORK DEVELOPMENT

Based on the Zachman EA framework, strategic alignment and governance is an integral part of security in developing an enterprise security framework, and all security needs for data, application, and technology dimensions need to derive from business (Fumy & Sauerbrey, 2006; Sherwood, 2005; Zachman, 1987).

Proper alignment of business security needs and security technology supports organizations to gain competitive advantages, and assists organizations to generate a higher return from its technical investment as compared to those which have a misalignment of business and technology (Ross, 2003). Developing enterprise plans with well-designed strategic alignment can guarantee a certain degree of quality, and can consequently reduce implementation error or unexpected events from happening, as well as increase the likelihood of successfully implementing projects without delay to gain benefit from project investments (Kearns & Sabherwal, 2006).

From governance perspectives, the top-down and centralization of decisions is the most effective governance approach to managing architectures for value (Kearns & Sabherwal, 2006; Ross, 2003). An efficient and effective governance ensures that organizations are compliant with comprehensive enterprise plans, and eventually perceive IT security business value.

From a security perspective, security policy is a starting point for securing organizations. Security policy is designed to define how organizations protect and maintain the confidentiality,

integrity, and availability of data resources, information systems, and network resources (Harris, 2005). In addition, developing security policies ensures compliance with external and internal requirements. External requirements are derived from laws and regulations for specific industries. Internal requirements can not only be derived from the organization's business objectives, mission, and policies, but can also be derived from the need to reduce risks, avoid disasters, or comply with standards, such as ISO 27000, CoBit, and ITIL. Another benefit of developing and maintaining security policies is in demonstrating the practice of 'due care' and 'due diligence' (Harris, 2005) within organizations.

To successfully develop and implement security policies, top management needs to be involved in and strongly support the project (Lam, 2005). A proposal with a report of external and internal requirements and a draft assessing budget can easily persuade managers to support the development and implementation of a security project. Having management support and authorization can resolve money and time issues. These managers can allocate the required budget and allow sufficient time for development and implementation. In addition, top management has power to affect processes by requiring employees to participate (Kearns & Sabherwal, 2006).

Why Developing Security Policies

Many security policy developers know the "how to" part, but always fail in the "why for" part in developing security policies (Hansche, Berti, & Hare, 2004). There are a few reasons for this situation. First of all, top management may not offer strong support to develop and implement security policy. In this case, top management may think that security policies are just statements. They may not want to commit too much time and money for developing and implementing the security project. The result is that top management or decision makers do not allocate enough budget and time to development and implementation teams. Secondly, the leader and team members of development and implementation teams may not believe that this security project is worthy of completion. Hence, they may just perform the minimum work that is required, such as only documenting security policies. Third, the top project manager's leadership may not be strong enough to successfully develop and implement security policies for the entire organization (Fedor, Ghosh, Caldwell, Mauarer & Singhal, 2003).

Some actions can be taken to prevent the above from happening. It is useful to emphasize the legal requirements, risks to the organization, and costs to be incurred. Educating or training top management or decision makers to strongly believe in the usefulness that security policies have to an organization is also a good idea, but may be harder to do. The team in charge of the security policies project should have a strong understanding of the security needs, and the leader should be carefully chosen. Criteria for selection of a leader should not only be based on hard skills but also on soft skills. Strong soft skills can save a lot of effort in making a security policies project successful.

How to Implement Security Policies Successfully

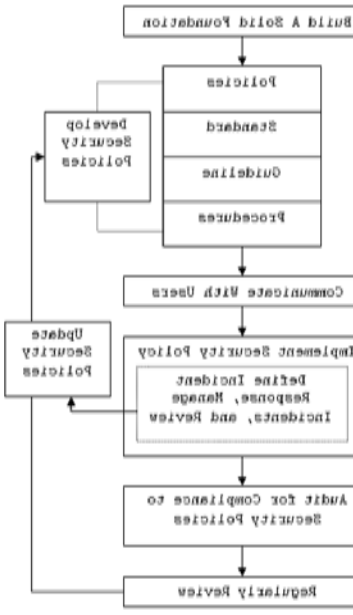
The implementation phase probably is the hardest phase in the life cycle of developing and maintaining security policies. Many organizations fail in this phase. To effectively and efficiently implementing security policies, teams first need to resolve many issues. Lack of

strong management support (Fedor et al., 2003; Lam, 2005), lack of budget (Kearns & Sabherwal, 2006; Martin, Pearson, & Furumo, 2007), lack of implementation time (Walker & Cavanaugh, 1998), lack of strong leadership (Fedor et al., 2003), lack of awareness of benefits of implementing security policies—"why for" (Hansche, Berti, & Hare, 2004)—, or ineffective communication with users (Jackson, Chow, & Leitch, 1997; Walker & Cavanaugh, 1998) may cause problems. Resolving all of the above issues can help in successfully implementing security policies.

The Role of Security Framework in Zachman EA Framework

The Zachman EA framework is one of the top-down approaches. Developing and maintaining security policy is achieved from a top-down approach. Figure 1 illustrates the role of security framework in Zachman EA framework.

Figure 1: The life cycle of the Zachman EA framework and security framework derived from (Sherwood, 2005; Spewak, 1993; Walker & Cavanaugh, 1998).



INFORMATION SECURITY INCIDENT MANAGEMENT CASE STUDY

This section illustrates the gap analysis of the L system in an information security incident management for one chosen organization and suggests a best practice model of information security incident management using ProVison (Metastorm, 2008). The organization recently set a goal to be compliant with security standard ISO 17799 2005. The scope of the case study is the L system, concentrating on analyzing information security incident management. The target of this case study is the compliance of this aspect with ISO security standard.

The first step is the assessment of the current state. Conducting questionnaires of information security incident management, based on the business model of the organization, and interviewing IT personnel are necessary for gathering the data needed for this case study. The questionnaire

focuses on whether there are procedures of reporting information security events and their weaknesses and on whether there are procedures for managing information security incidents and on potential improvements.

The result of performing gap analysis will be presented by graphic charts only. This graphic chart also can illustrate how easily weaknesses, strengths, and Critical Success Factors (CSFs) can be identified for planning future potential / candidate projects.

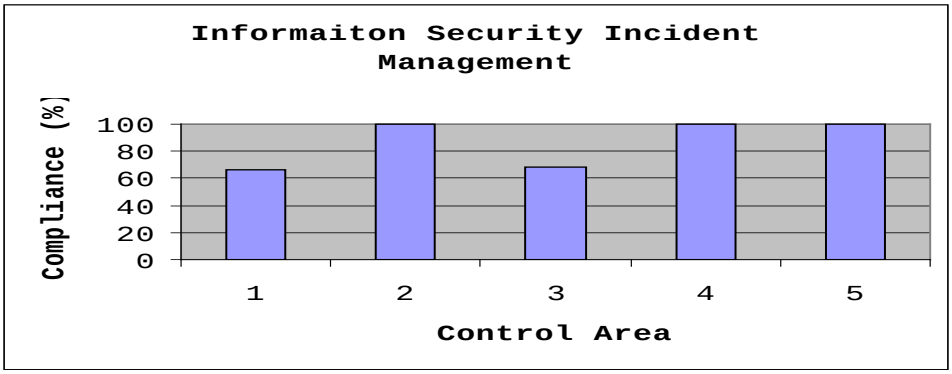
In figure 2, the X-axis lists control areas for information security incident management. The number represents different control areas. Table 1 depicts these control areas. The Y-axis represents the percentage of compliance with ISO 17799 2005, based on the results of the questionnaire. The number '0' indicates that nothing has been done while the number '100' represents full compliance with the ISO security standard. A low percentage of compliance with the ISO security standard indicates that there is high likelihood of security threats. If percentage of compliance is lower than 50, those control areas require immediate attention. All percentages of compliance for each control area is presented in Table 1 as well.

Table 1: Information Security Incident Management.

Control Area	Information Security Incident Management	Percentage of Compliance
1	Reporting information security events	66.67
2	Reporting security weaknesses	100.00
3	Responsibilities and procedures	68.75
4	Learning from information security incidents	100.00
5	Collection of evidence	100.00

Figure 2 shows that information security incident management has been well controlled. All five control areas are more than fifty percent compliant with ISO 17799 2005. Three out of five have one hundred percent compliance with the industry security standard (strength). This shows that the organization can quickly respond to some expected or unexpected events and can effectively take the right actions in response.

Figure 2: Information Security Incident Management.



The next step is to develop best practice models for the organization using ProVision based on the enterprise security framework illustrated in Figure 1. These best practice models address CSFs, which is a weakness in this example. From the table and bar chart (See Table 1 and Figure 2), 'reporting information security events' and 'responsibilities and procedures' only have about 66% to 69% of compliance with the ISO security standard. The main reason for the low percentage of compliance for the former case is the lack of a formal security incident response policy, which describes how events are to be reported. The organization only has a security standard and a process for responding to security incidents.

The recommendation here is to develop a formal and written security incident response policy. Figures 3, 4, and 5 illustrate a best practice security framework, followed by the best practice for developing a security policy, and finally a flow for effectively implementing one of the security policies. By following these strategies, the organization will be able to develop useful security incident management policies. For the latter one "responsibilities and procedures", the main reason for the low percentage is lack of well-documented guidelines for the complete cycle of responding to and handling incidents. Well-written guidelines can easily identify the responsibilities of each role of responding to and handling incidents, and can provide a clear guideline for managing incidents.

Figure 3: Security Framework.

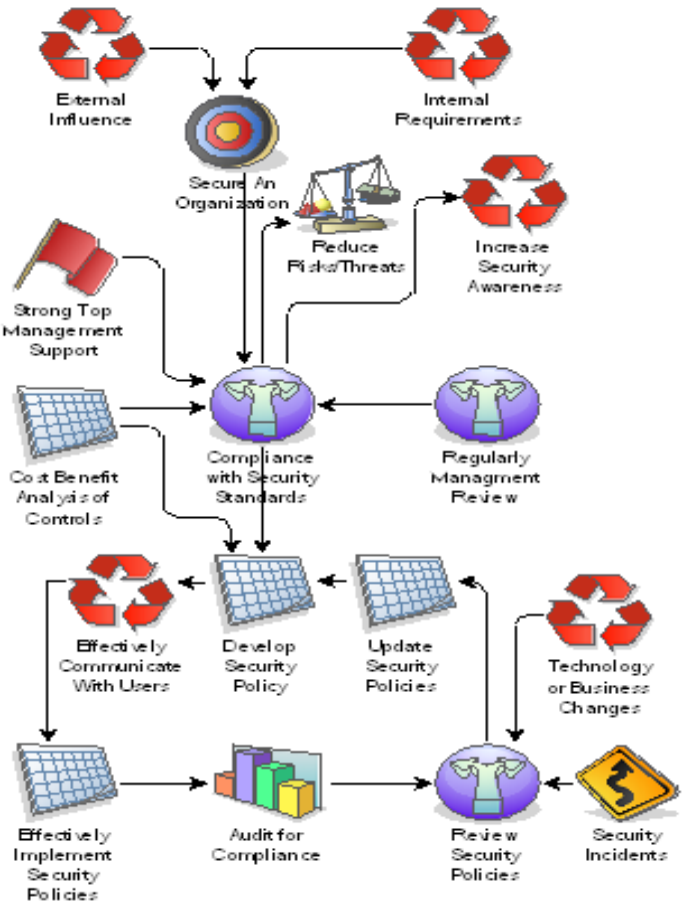


Figure 4: Develop Security Policy.

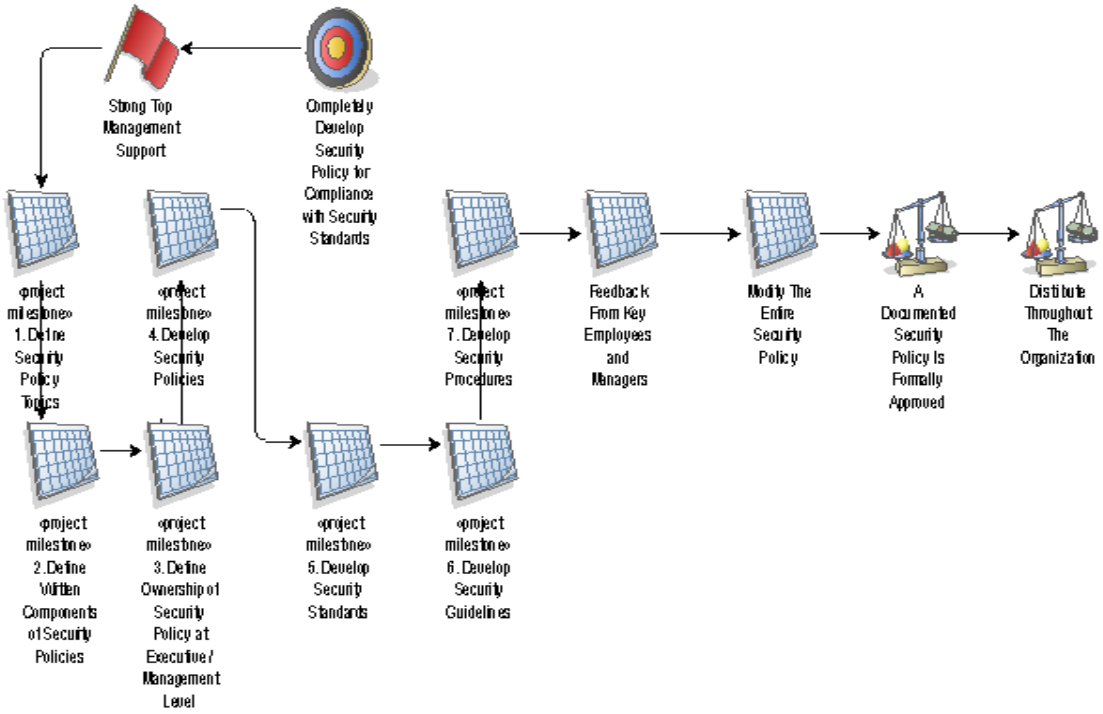
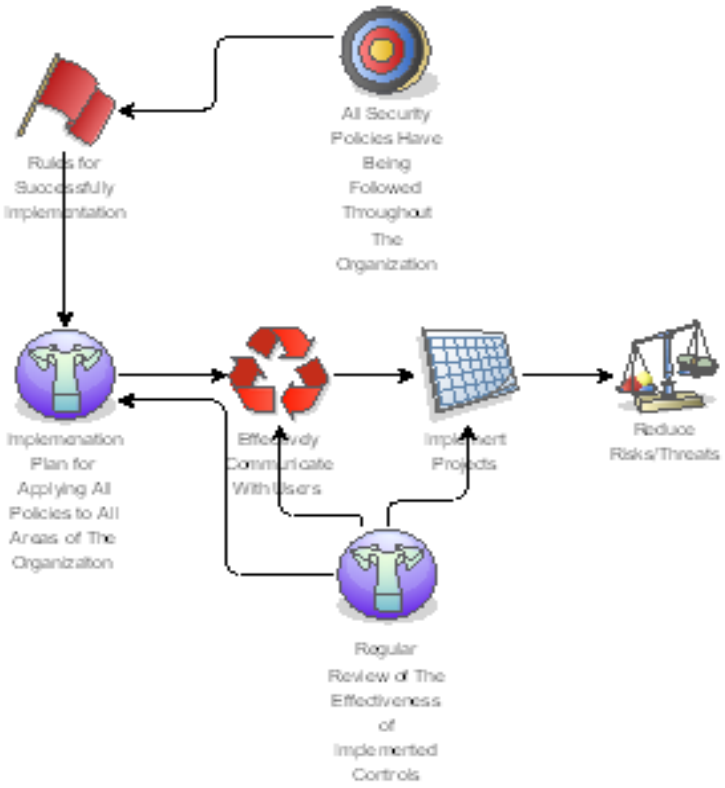


Figure 5: Effectively Implement Security Policies.



Figures 6, 7, and 8 illustrate the best practice strategy for a security incident response policy, followed by a presentation of the main scope of incident response policy in L system, and finally the best practice workflow. The workflow demonstrates proper management of a security incident scenario. One of essential steps for improvement is to follow written guidelines for responding to incidents to ensuring a quick, effective, and orderly response to information security incidents. In addition, determining and implementing countermeasures are recommended for preventing the same incident from happening again (Harris, 2005; Walker & Cavanaugh, 1998). After this step, all information relevant to the incidents should be documented, including what the incident is about, the impact of the incident, the method by which it should be handled, how to prevent it from happening again, and so on. The last step should also include a review of the security policy and allow for modifications if needed. This scenario not only can well handle security incident correctly and efficiently, but also can ensure the same incident will not happen again in the future.

Figure 6: Strategy for Security Incident.

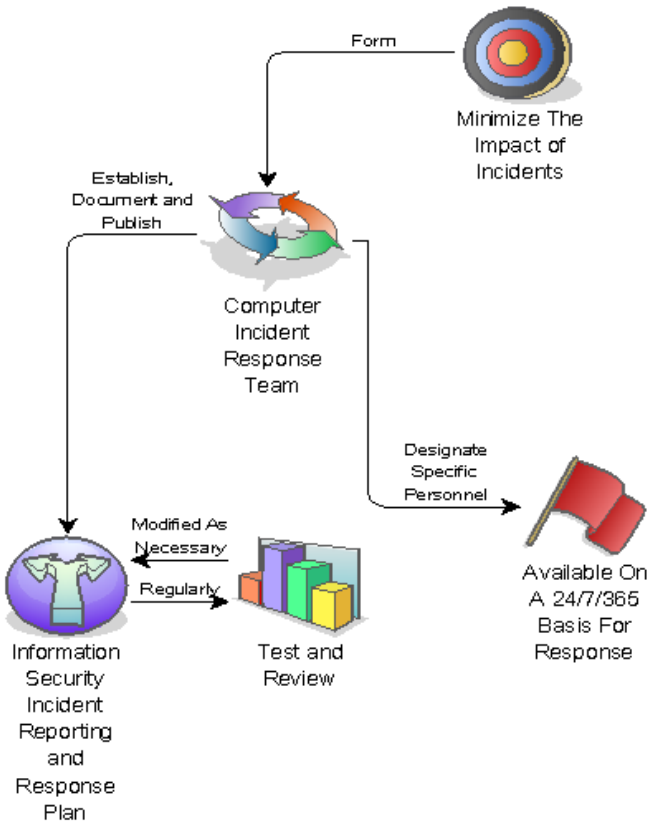


Figure 7: Security Incident Response (L System) Response Policy.

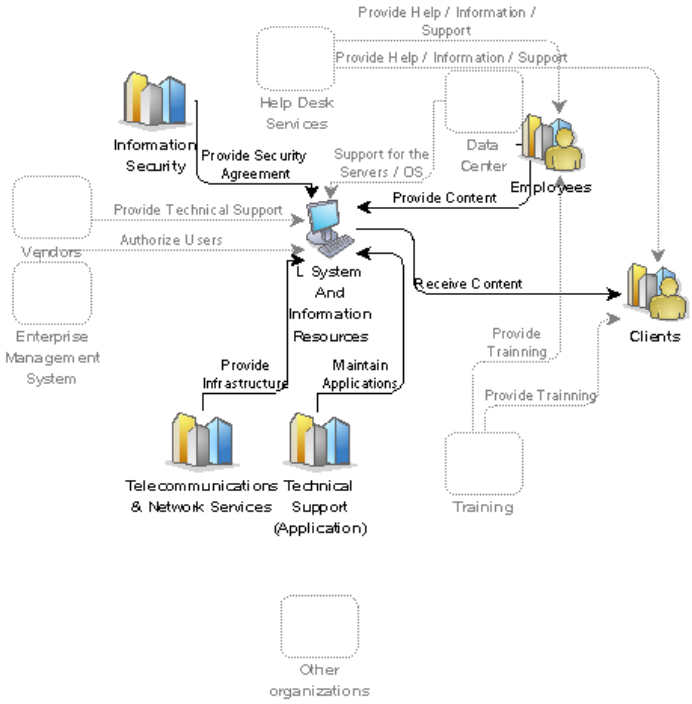
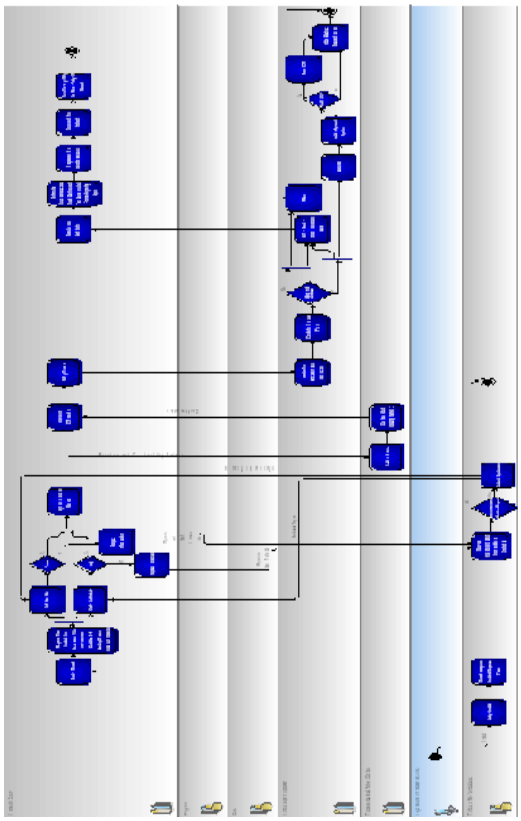


Figure 8: Workflow of Security Incident Response (L System).



CONCLUSION

Security is important for all organizations, especially for large enterprises. Inappropriate security management can allow critical events to threaten an organization's bottom line through the loss of reputation, customers' trust, fortune, confidential information, and so on. Incorporating a security dimension to the Zachman EA framework is a good practice for efficiently and effectively securing an organization's IT. Zachman's EA framework is a blueprint for all organizations. It allows development teams to align business and IT security, and to transform business needs into IT security business value. Well-developed plans can have a positive affect on the quality of implementation and produce fewer unexpected implementation errors. Strong top management support and applying top-down governance helps to deliver value to the organization through development and implementation. Strong top management support means not only "approval" of sufficient time and budget, but also involves getting top managers to participate. These top managers have power to enforce cooperation throughout their organizations which is instrumental to the success of these projects. Applying top-down governance not only improves the efficiently of the development of strategies and plans but also ensures that the organization conforms to well-developed plans. Top management can control and monitor the state of enterprise security with efficiency through a view of the organization as a single entity. All considerations must also be consistent within the entire enterprise. Top-down governance makes communication easy because, generally speaking, there are just two ways of communicating: top-down or bottom-up.

Applying the framework developed here can help organizations pinpoint security strengths, weaknesses, and CSF with ease. It can also help them develop the most appropriate security blueprint and implement regular cost-effective security projects with efficiency. These benefits of applying the enterprise security framework are demonstrated in the case study, which focus on information security incident management. In this case study, questionnaires and interviews were conducted and one-step risk assessment and analysis was applied for analyzing the gap. Gap analysis can help developers prioritize success factors and identify CSF for achieving security goals. Finally, a best practice model is suggested and developed using ProVision, which is based on CSF.

REFERENCES

Boh, W. F., & Yellin, D. (2006). Using Enterprise Architecture Standards in Managing Information Technology. *Journal of Management Information Systems*, 13(3), 163-207.

Farrel, R. J. (1996). ProVision (version 6.0.2) [Computer Software]. Baltimore: Metastorm, MD.

Fedor, D. B., Ghosh, S., Caldwell, S. D., Maurer, T. J., & Singhal, V. R. (2003). The Effects of Knowledge Management on Team Members' Ratings of Project Success and Impact. *Decision Sciences*, 34(3), 513-539.

Fumy, W., & Sauerbrey J. (2006). Enterprise Security: IT Security Solutions: Concepts, Practical Experiences, Technology. Berlin: Publics Corporate Publishing.

Hansche, S., Berti, J., & Hare, C. (2004). Official $(ISC)^2$ Guide to the CISSP Exam. London: Auerbach.

Harris, S. (2005). All-In-One: CISSP Exam Guide. California: McGraw-Hill Companies.

Jackson, C. M., Chow, S., & Leitch, R. A. (1997). Toward an understanding of the behavioral intention to use an information system. *Decision Sciences*, 28(2), 357-389.

Kearns, G. S., & Sabherwal, R. (2006). Strategic alignment between business and information technology: a knowledge-based view of behaviors, outcome, and consequences. *Journal of Management Information Systems*. 23(3), 129-162.

Lam, W. (2005) Investigating success factors in enterprise application integration: A case-driven analysis. *European Journal of Information* systems, 14(2), 175-187.

Martin, N. L., Pearson, M., & Furumo, K. (2007). IS Project Management: Size, Practices and The Project Management Office1,2. *The Journal of computer Information Systems,* 47(4), 52-60.

Metastorm (2008). Metastorm releases enhanced ProVision enterprise modeling suite. http://www.metastorm.com/news/2008/040208.asp

Ross, J. W. (2003). Creating a strategic IT architecture competency: learning in stages. *MIS Quarterly Executive*, 2(1), 31-43.

Sherwood, J. (2005). Enterprise security architecture: a business-driven approach. San Francisco: CMP Books.

Spewak, S. H. (1993). *Enterprise Architecture Planning: Developing a Blueprint for Data, Applications, and Technology*, Wiley, New York, NY.

Walker, K. M., & Cavanaugh, L. C. (1998). Computer Security Policies. Palo Alto: Sun Microsystems, Inc.

Zachman Framework. Retrieved July 14, 2007 from http://www.zifa.com/

Zachman, J. A. (1987). A Framework for Information Systems Architecture. *IBM Systems Journal*, 26(3), 276-292.

This Page Left Intentionally Blank