

Security Systems and the System Development Life Cycle

Brian D. Otte

Capella University

Table of Contents

Title Page ..... 1

Table of Contents ..... 2

Abstract ..... 4

Introduction ..... 5

Discussion ..... 5

    Assesses the Significance of New Developments in Security Systems and the SDLC.. 6

        The System Development Life Cycle—the Waterfall ..... 6

    Identifies and Evaluates the Current Thinking and New Developments in Security  
Systems and the SDLC ..... 8

        Planning ..... 8

        Analysis ..... 9

        Logical Design ..... 10

        Physical Design ..... 11

        Implementation ..... 12

        Maintenance ..... 13

Evaluates the Implications of Developments in Security Systems and the SDLC for Individuals and Organizations .....	15
Security Systems SDLC and Business Strategy .....	15
Alignment of IT Strategy and Business Strategy.....	15
Security and Alignment of IT with Business Strategy.....	16
Business Low-cost Strategy .....	17
Business Differentiation Strategy .....	17
Business Niche or Focus Strategy.....	18
Current Research.....	19
Assesses Opportunities for Further Research Concerning a Specific Aspect of Security Systems and the SDLC .....	20
Conclusion .....	23
References.....	25

### Abstract

Organizations implement security systems to protect their assets. An organizational strategy determines the attributes which a security system possesses and also determines the methods whereby these systems are implemented, maintained, and used. Organizations have choices which they can make during these phases which have been shown to aid or hinder the process depending on the strategy of the organization. Through this literature review, specific considerations specific to security systems are presented within the System Development Life Cycle with respect to business strategies of low-cost, differentiation, and niche. Linking scholar and practitioner research with respect to security systems throughout the System Development Life Cycle is identified as lacking and a call for more research in these areas is presented.

## Introduction

Organizations find computers useful for many reasons as they enable efficient processing of the organizations assets and information. Small organizations as well as multi-national corporations find similar efficiencies in using computers to automate their data manipulations. As organizations grow from small organizations to larger organizations the ease of implementing new software systems becomes more difficult. To mitigate these difficulties, organizations follow a methodology called a System Development Life Cycle (SDLC) when managing their information systems (Hoffer, George, & Valacich, 2008). Many derivations exist of the SDLC, some are more appropriate and are aligned with business strategies than others and focus on different aspects of implementing systems. This article assesses the end to end process of delivering security systems within an organization. This is accomplished through an examination of new developments derived from a literature review conducted from recent research in delivering security systems through a waterfall SDLC.

The literature review focuses on the evolution of the end-to-end Information Technology (IT) delivery process with respect to systems which deal with security through what is currently the state of the art thinking about how the end-to-end IT delivery process should be done. Through this research, opportunities have been uncovered for further research, and these points are also examined specific to implementing security systems within the SDLC.

## Discussion

*Assesses the Significance of New Developments in Security Systems and the SDLC**The System Development Life Cycle—the Waterfall*

The SDLC is a grouping of steps which organizations use to deliver Information Systems. Most organizations subscribe to some approach of SDLC for delivering IT systems; the traditional approach is the waterfall (Hoffer, George, & Valacich, 2008). This approach, as presented by Hoffer, George, and Valacich, contains six phases each culminating when reaching a milestone and then cascade to the next phase. These phases, in sequential order are: planning, analysis, logical design, physical design, implementation, and maintenance. The waterfall method is presented as a general framework to present the special considerations of implementing security systems as a useful framework in development of IT systems.

Some criticisms of the waterfall model are presented by Hoffer, George, and Valacich (2008) who believe that organizations associate dates to milestones as a method to measure success. According to Hoffer, George, and Valacich “The focus on deadlines results in systems that do not match users’ needs and require extensive maintenance, unnecessarily increasing development costs” (p. 18). These development costs are extended throughout the system life if not properly addressed by the developer. For example, improperly rushing a project through the critical phases where analysts obtain user requirements will undoubtedly cause increased issues in the maintenance phase forcing the project developers to fix what was rushed earlier in the project. Problems which are discovered later in the development process are more expensive and require more time to fix than if they are discovered earlier in the process (Wu, 1992). Wu suggests that additional effort is required earlier during the planning and analysis phases, which will lower costs in the maintenance phase. Hoffer, George, and Valacich cite Dorfman and

Thayer reporting that maintenance costs are 40 to 70 percent system development costs (p. 18). Focusing on deadlines, as opposed to the project content is one issue which Hoffer, George, and Valacich present as problematic with the waterfall SDLC. Choosing a SDLC which complements the organizations strategy will also aid in the development of the project.

There are as many criticisms of system development methods as there are methods. Security systems also impose additional considerations which need to be taken into account during the process. For instance Boehm (2006) discusses some of the criticisms of agile teams with respect to security. Boehm presents a view, specifically concerning security, with agile teams that overlook important details early in the development life cycle intending to address the issues later in the process. As Wu (1992) presents this causes additional time and money to be invested in the process. This causes problems for the agile teams because developers find it difficult to secure a system which is hastily chosen and inappropriate finding too late that the system is un-securable (Boehm, 2006).

Many different SDLC methods can be used. An organization should choose a SDLC which works for what it needs to have work. Therefore this article will not attempt to present one view of the right SDLC, but rather cover special methods which can be used within any SDLC. Rather than compare individual SDLC processes, individual aspects which are germane to security systems are presented through the traditional waterfall SDLC.

Within the waterfall SDLC phases, research has provided additional frameworks which take special consideration to ensure that security is implemented with a level of strategy which is optimal. The following presents research which deals with security during each phase of the SDLC. The first phase in the Waterfall model of the SDLC is the planning phase.

*Identifies and Evaluates the Current Thinking and New Developments in Security Systems and the SDLC*

*Planning*

The planning phase lays the ground work for the whole project. Security systems have unique aspects which need to be dealt with at each phase of the SDLC, and Devanbu and Stubblebine (2000) believe that organizations should select "...an appropriate security policy and model [which] is best done early in a product's lifecycle. The challenge is to integrate security requirements analysis with the standard requirements process" (p. 228). The planning phase is appropriate to integrate the special considerations which apply to security systems in the form of extra precautions and security requirements which are needed for the project. The options which an organization should pursue in the planning phase are presented

According to Whitman and Mattord (2005) who discuss the security SDLC, unique aspects related to implementing security systems in this phase are stated as "Management defines project processes and goals documents in the program security policy" (p. 25). The planning phase, like all phases of the SDLC, requires that the organizational strategy be clearly understood by system developers as they are integrating a system which reflects and enforces the strategy the organization is adhering to.

Kao and Decou (2003) present a framework, which is placed within the planning phase, which places strategy at the core of their model. Whether the organization is seeking a security system which will enable an online presence or the security system will support traditional business model, the application of a consistent strategy is extremely important. Porter (2001) suggests that organizations need to be consistent with both traditional business strategy and their

Internet strategy stating that “In many cases, the Internet complements, rather than cannibalizes, companies' traditional activities and ways of competing” (p. 73). This is reinforced by Kao and Decou who believe that successful analysis of seven critical dimensions is imperative and aligned with the organization's strategies which are: finance, legality, logistics, marketing, operations, security, and technology (p. 245).

Specifically addressing security in the planning phase Kao and Decou (2003) are interested in ensuring that the organization utilizes adequate security and have reassuring policies in place to protect its customers (p. 250). Two awareness issues during the planning phase exist for the organization concerning security which deals with protecting the transfer of information, and ensuring that the repository of information remains secure (Kao & Decou).

### *Analysis*

According to Whitman and Mattord (2005) who discuss the security SDLC, unique aspects related to implementing security systems in this phase is that system analysts need to consider existing policies and programs, current threats and controls, legal issues, and perform a risk analysis (p. 25).

Devanbu and Stubblebine (2000) believe that functional requirements within the SDLC are managed in a rational manor, but believe that “security requirements have not typically received the same type of careful analysis” (p. 228). Devanbu and Stubblebine believe that “...systems engineering must be unified with security engineering” (p. 228). When organizations are conducting an analysis, additional care and concern needs to ensure that the security system adequately mitigates the potential threats which they are designed to mitigate. Devanbu and Stubblebine call for “...security engineers to develop applicable threat models, and

select those security measures that are most needed for market success” (p. 228). One view is that the analysis phase is part of the security system itself. The system carries out the logic which the analyst determines appropriate. In other words a system which monitors itself and reports the status of security through some predetermined mechanism.

### *Logical Design*

According to Whitman and Mattord (2005) who discuss the security SDLC, unique aspects related to implementing security systems in this phase include developing a security blueprint, plan for incident response, define what the businesses response is to a disaster, and determine through a feasibility study if both the project should continue and/or if the project should be outsourced (p. 25)

Devanbu and Stubblebine (2000) call for changes in software architecture which aid better security in software. Specifically Devanbu and Stubblebine see two main issues with security and logical design: Legacy security mismatches, and separating the security aspect.

Legacy security mismatches, according to Devanbu and Stubblebine (2000), exist as different security architectures apply security differently. An example given is where UNIX uses username and password authentication which grants system authorization based on membership of three groups called user, group, or world. CORBA, on the other hand, uses Kerberos which uses credentials which are owned by the CORBA client (Devanbu & Stubblebine, p. 229). One method which Devanbu and Stubblebine present is encapsulation of these authorizations methods and unifying the security methodology.

Separating the security aspect deals with legacy systems, which according to Devanbu and Stubblebine (2000) “...is the difficulty of identifying the code that is relevant to security,

changing it, and integrating the changes back into the system” (p. 230). The code, which is identified as security related is modularized by separation which allows for standardization. Through this process Devanbu and Stubblebine assert that “security features would be easier to isolate and maintain” (p. 230).

Both of these deal with an understanding that the developer has about the system which they are working on. Plugging into a system without understanding the nuances associated with interacting with a system is a risk which both legacy security mismatches and separating the security aspects address. However, an organizational strategy which unifies either of these two components minimizes the risk associated from a security perspective. Homogenous and modularized authentication and authorization at both the system and application level deal with the issues presented by Devanbu and Stubblebine (2000), which are driven by an organizational strategy.

### *Physical Design*

According to Whitman and Mattord (2005) who discuss the security SDLC, unique aspects related to implementing security systems in this phase is that analysts select technology from security blueprint, define the meaning of success, design physical security, and review and approve the project (p. 25).

Devanbu and Stubblebine (2000) call for “...API calls, to ‘simulate’ attacks on a program and attempt to expose vulnerabilities” (p. 235). This requires the formulation of these APIs and thorough testing of their viability. Additionally, strict control of these APIs is important, should these be reverse engineered the checking ability which the developer uses could be divulged

putting proprietary security control mechanisms into the public view, making these API's themselves an additional security threat.

Physical design similar to logical design requires modularization of code. One method which an organizational strategy aids the implementation of modularization is through the use of CASE tools to aid the development process. According to Hoffer, George, and Valacich (2008) CASE tools "...enable the automatic generation of program and database definition code directly from the design documents..." (p. 20). The automatic generation of code enables the developer to ensure that the same mechanisms are used for authorization and authentication throughout the organization.

### *Implementation*

According to Whitman and Mattord (2005) who discuss the security SDLC, unique aspects related to implementing security systems in this phase is that analysts need to buy or develop security system, and present the tested system to management for approval (p. 25).

Devanbu and Stubblebine (2000) present research which details some issues which concern implementation and the SDLC. Specifically, Devanbu and Stubblebine inform that incompatibilities exist between software packages which have security implications. Incompatibilities and the issue of software updates throughout the implementation phase add to the complexity of security and implementing software. Devanbu and Stubblebine state that "...users are often asked to update and re-configure their systems in response to announced threats (e.g., viruses) and newly discovered vulnerabilities" (p. 235). Updating or patching of users systems, who are often mobile and remote from the main office, is an important component of an organizations security. This is reflected in research as Ciampa (2004) presents information

about the time delay which exists between when patches are released, to fix known vulnerabilities, and when the viruses begin to attack the systems (see Figure 1).

Name of Attack	Patch Issued	Attack Begins	Days
Nimda	10/17/00	9/18/01	336
Code Red	6/18/01	7/19/01	31
Blaster	7/16/03	8/11/03	27

Figure 1. The gap between patches and virus attack (Adapted from Ciampa, 2004).

Users performing technical tasks or manual tasks are not a good strategic move for organizations on many levels. The primary problem is that performing some of these technical tasks requires elevated privileges on the user's system and by itself present inherent security issues. In addition to the issues of dealing with these updates, according to Devanbu and Stubblebine users might be prone to social engineering exploits where users divulge personal or private information (p. 235). These processes are inconvenient for the user and open the organization to additional security issues.

### *Maintenance*

According to Whitman and Mattord (2005) who discuss the security SDLC, unique aspects related to implementing security systems in this phase is that an analyst should "Constantly monitor, test, modify, and repair to meet changing threats" (p. 25).

Devanbu and Stubblebine (2000) present research which details some of the concerns with respect to security during the maintenance phase of a SDLC. Following the deployment of security systems, errors or issues with the system might be discovered. Some scenarios are that

the vendor has fixed an issue, or some functionality of the security system requires modifications. Security systems are not static systems and may require that additional functionality is provided which requires system modification. Devanbu and Stubblebine call for controlled delegation of administration and privacy protection.

Controlled delegation of administration refers to administration which is aware and understands which sources are trustable, and which sources of information are not. This is an understanding of security and an understanding of what information is pertinent and applicable. It is not just enough to seek out security information, but to understand what the security information means in context of the current business strategy and the current security system, applying the information when both business strategy and the current security system deem that modifications are required. Therefore many are aware of changes to a system, but no one individual affects these changes. This allows for an audit trail to understand when something happened and how the change was implemented.

Privacy protection refers to keeping credentials and the identity of the administrative users from general knowledge. Devanbu and Stubblebine infer that this is a system which is setup to manage the protection of privacy (p. 236). Privacy protection also implements a system which requires more than one control mechanism to implement or change a security system. By keeping the management of these security systems as privileged information the minimization of social engineering exploits is also minimized.

*Evaluates the Implications of Developments in Security Systems and the SDLC for Individuals  
and Organizations*

*Security Systems SDLC and Business Strategy*

The business strategy is an important concept to understand in order to align with its strategy. For an organization to get the most it can from IT, both the business strategy and the strategy of IT need alignment. A strategy concerns the choices made and the methods used to accomplish a task. As an analogy, Microsoft Windows allows a user to use different strategies to navigate its Windows operating system to accomplish a task. Some users exclusively use the mouse where other users like keyboard shortcuts and some find themselves using a combination of both depending on the situation. So a user can adopt any number of navigation strategies to do accomplish a task using Microsoft Windows. Similarly, there are options as to how IT chooses the investments it makes. Organizational resources are maximized when business and IT strategy are aligned by prioritizing investments that an organization makes in IT to support the business functions (Ward & Peppard, 2002). A strategy which is in alignment achieves more than an organization which is out of alignment.

*Alignment of IT Strategy and Business Strategy*

Implementing security systems requires special consideration in the SDLC as presented through the waterfall SDLC, and requires additional consideration through each phase. These additional considerations are applicable to organizations whose business strategy deems them important. Understanding the business strategy is mandatory to ensure that IT strategy is in alignment. Ward and Peppard (2002) support this by stating “[a]ll organizations have some form

of strategy, whether implicit or explicit, and the essence of business strategy lies in creating future competitive advantages faster than competitors” (p. 65). Aligning IT processes with business processes seeks to create a competitive advantage and implement the advantage faster than competitors. Research indicates that specific methods within the SDLC have shown to successfully be applied to delivery of security systems. Organizations which employ these methods when delivering security systems through the SDLC, receive the strategic benefits of the implementation of security systems.

Jeffery and Leliveld (2004) offer stages of IT management teams with respect to alignment of investment portfolio and business strategy. According to Jeffery and Leliveld “...companies use evolving metrics to measure a project’s value through its life cycle” (p. 44). IT project management which is aligned with the business model directly affects the organizations balance sheet. Jeffery and Leliveld state that “A statistical link [exists] between a synchronized ITPM process and return-on-asset (ROA) performance” (p. 45). Aligning the ITPM process with respect to security systems allows an organization to minimize redundancies, which by themselves increase security, as well as providing the services which fits an organization’s needs.

### *Security and Alignment of IT with Business Strategy*

The business strategy is defined by management which also defines the processes within the organizations that enable that strategy. Alignment of IT with the business strategy benefits the organization by creating synergies and processes which reinforce the strategy. Three generic business strategies presented by Ward and Peppard (2002) are low-cost strategy, differentiation strategy, and niche or focus strategy.

### *Business Low-cost Strategy*

A business can adopt a low-cost strategy through what Ward and Peppard (2002) call cost leader. Through this strategy organizations attempt to identify activities within the business and minimize the expenses associated with them (Ward & Peppard, p. 108). Information systems within this business strategy deal efficiently with basic information processes, force user adherence to conformity, and seek to add value by increasing efficiency (Ward & Peppard, p. 108). Security systems in this regard must ensure that the data is protected while ensuring that the most efficient cost effective system is employed. Enabling features beyond defined requirements are not part of the strategy and the system which is at lowest cost which meets requirements is always the right choice.

Haley, Laney, Moffet, and Nuseibeh (2008) presents a framework which is viable in all stages of the SDLC and brings value to the organization for business which adhere to the low-cost strategy, by ensuring, and mandating that security provides a service at the best price. Haley et al. state “One must be able to connect specific development and operational expense to the requirements being satisfied in order to determine cost/benefit information” (p. 134).

### *Business Differentiation Strategy*

Innovation and creativity signal a differentiation strategy as Ward and Peppard (2002) discuss an organization whose focus on the market is through the creation of a strong brand and by focusing on incentive schemes for the people within the organization (p. 109). Ward and Peppard believe that Information Systems within an organization that uses the differentiation strategy attempts to derive value from IT by doing new things or doing existing things better (p.

109). Additional features which enable different aspects of accessibility are part of this strategy and technologies which enable customer satisfaction are deemed appropriate even if they cost more to introduce.

The framework presented by Haley et al. (2008) also applies to the differentiation strategy as this framework provides and even mandates flexibility to ensure that security requirements are consistently applicable to the needs to the organization and individuals through its iterative processes during the maintenance phase.

#### *Business Niche or Focus Strategy*

A niche or focus strategy, in addition to specializing in delivering and maintaining a specialized feature in the market, according to Ward and Peppard (2002) also adopts a low-cost or differentiation strategy. Organizations which adhere to this strategy will use IT to address the needs of their targeted market, and ensure that the processes that IT supports produce a clear cost advantage over the competition (Ward & Peppard, p. 110). Identifying the customer base is absolutely required, while addressing that customer base through applicable technology adds value to the organization. Additional features which appeal to the identified customer base is appropriate. The key aspect with this business strategy is to understand the target audience, and design security systems with respect to their needs.

The recommendation for niche or target strategy is to address the needs of the target audience, and then as Haley et al. (2008) presents, then use a low-cost or differentiation strategy. For security systems the same applies, focus on the target or niche first, and then adopt a low-cost or differentiation strategy applicable to the security system.

*Current Research*

Previous research by Devanbu and Stubblebine (2000), present a detailed inspection of the SDLC with respect to security and place the unique needs associated with implementing security systems within the SDLC. Current research presented Haley et al. (2008) present a framework with details security requirements and analysis which provides the developer a mechanism to understand if the requirements have been met as stated in the definition of the security system and allows the implementation of the security system to progress through the SDLC model. Haley et al. presents an iterative framework which suggests that four phases are applicable to security systems as: identify functional requirements, identify security goals, identify security requirements, and construct satisfaction arguments. These tasks primarily exist in the planning, analysis, logical design, and physical design phases of the waterfall SDLC.

Security systems, when implemented should perform the desired function and protect the organizations interests. However, security system function requires adaptability, and Haley et al. (2008) provide mechanisms for organizations to contend with the implementation and maintenance phases of the waterfall SDLC. Implementing systems, which replace older systems, requires removal and replacement of the older system. Appropriate measures need to be taken with respect to removing the old system. According to Haley et al. assumptions by software analysts is that once a system is taken out of service the system is no longer in a hostile environment. Haley et al. suggest that executables on the system can be analyzed and exposed. Systems which contain similar architecture, even though not currently functioning as a production security system, might reveal information which provides a mechanism to enable unauthorized access discovered though a weakness of the older system. Therefore appropriate

measures ought to be taken to ensure that older systems are disposed of in a manner which does not reveal sensitive methods or vulnerabilities.

As stated earlier, Haley et al. (2008) presented a process which is iterative, and if applied to security systems in the maintenance phase, provides adaptability for new dynamic security threats which present themselves after a security system is put into service during its functional life. Haley et al. presents two scenarios a systems analyst might use to determine the actions a security administrator should use during different risk analyses.

An analyst might determine, through risk analysis, that identifying a breach and recovering or repairing the breach is more cost effective than preventing the breach. This perspective requires active interaction between the system and an administrator throughout the maintenance phase. The second scenario details the active monitoring of the effectiveness of the identifying mechanism by the systems administrator, and is required throughout the maintenance phase (Haley et al., p. 136). Therefore, the system must determine the potential for a breach, and the determination mechanism which the system uses needs to be validated throughout the maintenance phase of the security system.

*Assesses Opportunities for Further Research Concerning a Specific Aspect of Security Systems  
and the SDLC*

Scholar research dealing with security and security systems exists as fragments within SDLC and rarely exists as the main focus throughout the whole of a SDLC. Abstractions and theories, while valuable for academics for generating theories, do little to help organizations and their analysts understand the special issues which surround and end to end delivery of security systems.

Practitioner research is extensive but only deals with specific phases of the SDLC such as implementation, maintenance, or monitoring. Another issue is the heavy representation of implementation research of security systems composed by vendors delivered with the focus on bolstering support for their products. Besides the inherent bias, this research is either skewed by vendor, focused on getting the product into an organization, or limited to one type of security system which is only adequately represented to the implementation phase. For instance Ciampa (2004) presents Microsoft and Cisco's view on security which is Secure by Design, Secure by Default, and Secure by Deployment (p. 169). The research discussion does not effectively deal with what other research has shown to be the most expensive phase which is the maintenance phase (Wu, 1992) (Hoffer, George, & Valacich, 2008). Each of these issues renders the available research by scholars and practitioners as inadequate in an end to end delivery of a security system.

A need exists for useful research throughout the SDLC which is both based on theory and applicable to real security and security systems. The focus of this research needs to concentrate on an end to end delivery of security systems based throughout the whole SDLC. Scholar research needs to move along the theoretical/practical continuum and link theory to specific vendor offerings. Practitioner research needs a wider view, beyond the implementation phase, dealing with the dynamic nature which security systems require during the maintenance phase. The resultant research requires a merging of scholar research with the practitioner research, and is needed to aid organizations that desire an understanding of best practices for security systems throughout the SDLC.

The implications for the SDLC, with respect to security systems, are that special processes need to be utilized with security systems. Organizations need to have an understanding that security systems need additional care and concern related to their functioning throughout the SDLC. The ability for organizations to determine the appropriate level of security is determined from the business strategy and may change throughout the SDLC requiring additional steps to ensure effective implementation of security systems. Research into the additional steps and the effect on the SDLC depending on the business strategy is required for organizations to understand the alignment steps.

The evaluation of implementing security and security systems within the SDLC also has significance for the individual. Special handling of security systems is recommended throughout the life of security system. This information manifests itself in the research which documents the “hardening” of Commercial Off the Shelf (COTS) systems (Fraser, Badger, & Feldman, 2003). At the individual level, those responsible for security need awareness for this special handling for COTS software, which occurs throughout the life of a security system, affecting each phase of the SDLC for the individual.

Organizations are faced with unknowns when implementing new systems. The security SDLC as presented by Whitman and Mattord (2005) guides organizations through an implementation process utilizing a methodology to discern what is unknown and address these issues. When dealing with security and security focused systems, an understanding of how much security needed is appropriate. Identifying and addressing these special circumstances within

each of the phases of the SDLC is appropriate and an analysis of current research enables an assessment of the significance of new developments in the delivery process of security systems.

### Conclusion

This literature review has presented a view which exposes two voids in existing research. The first void exists with respect to practitioner research and manifests itself as a deficiency of research throughout the whole SDLC, and is especially lacking after the implementation phase. Practitioner research, which is usually linked to a specific product, does include linking products to a business strategy, but does not include products from multiple vendors.

The second void exists with respect to scholarly research and manifests itself through the linking of specific security related processes in the SDLC to the organizational strategy. Scholarly research avoids linking products from vendors to the theories provided and provides little help to organizations which desire to implement theoretical constructs to security systems.

These two issues need additional attention with respect to security systems and the SDLC. Practitioner research needs to address phases after implementation and scholarly research needs a method to link theory to specific products without introducing bias within their research. The purpose the research exists, both practitioner and scholarly, provides a mechanism for organizations to use and apply the information.

Security and security devices are continually adapting to new threats. Through this literature review organizations and individuals will gain an understanding that security systems are dynamic in nature throughout the SDLC and require flexibility within the businesses strategy.

This dynamic and flexible strategy enables the organization to benefit from the systems' use while maintaining a secure environment. Applying these special considerations for security systems throughout phases of the SDLC ensures a dynamic and flexible strategy, enabling individuals and organizations to succeed in delivering a security system which is in strategic alignment with the business strategy.

## References

Boehm, B. (2006). *A view of 20th and 21st century software engineering*. Paper presented at the Proceedings of the 28th international conference on Software engineering.

doi:10.1145/1134285.1134288

Ciampa, M. (2004). *Security Awareness: Applying Practical Security in Your World*: Thomson Course Technology.

Devanbu, P. T., & Stubblebine, S. (2000). *Software engineering for security: a roadmap*. Paper presented at the Proceedings of the Conference on The Future of Software Engineering.

doi:10.1145/336512.336559

Fraser, T., Badger, L., & Feldman, M. (2003). Hardening COTS software with generic software wrappers. *Foundations of Intrusion Tolerant Systems, 2003 [Organically Assured and Survivable Information Systems]*, 399-413.

Haley, C., Laney, R., Moffett, J., & Nuseibeh, B. (2008). Security Requirements Engineering: A Framework for Representation and Analysis. *IEEE Transactions on Software Engineering*, 34(1), 133. Retrieved May 1, 2008, from ABI/INFORM Global database.

Hoffer, J. A., George, J. F., & Valacich, J. S. (2008). *Modern systems analysis and design* (5<sup>th</sup> ed.). Upper Saddle River, NJ: Prentice Hall.

Jeffery, M., & Leliveld, I. (2004). Best Practices in IT Portfolio Management. *MIT Sloan Management Review*, 45(3), 41-49. Retrieved May 4, 2008, from Business Source Premier database.

- Kao, D., & Decou, J. (2003). A strategy-based model for e-commerce planning. *Industrial Management + Data Systems*, 103(3/4), 238. Retrieved May 1, 2008, from ABI/INFORM Global database. (Document ID: 346768491).
- Porter, M. E. (2001). Strategy and the Internet. *Harvard Business Review*, 79(3), 62-78. Retrieved May 31, 2008, from Business Source Complete database.
- Ward, J., & Peppard, J. (2002). *Strategic Planning for Information Systems* (3rd ed.). New York: John Wiley & Sons, Ltd.
- Whitman, M. E., & Mattord, H. J. (2005). *Principles of Information Security* (2nd ed.). Boston Massachusetts: Thomson Course Technology.
- Wu, R. (1992). The Information Systems Auditor's Review of the Systems Development Process and its Impact on Software Maintenance Efforts. *Journal of Information Systems*, 6(1), 1-13. Retrieved February 2, 2008, from MasterFILE Premier database.