CERIAS Tech Report 2010-28

Increasing Security Effectiveness in IT Enabled Products Using Balanced Scorecard Framework

by Anurag Jain
Center for Education and Research
Information Assurance and Security
Purdue University, West Lafayette, IN 47907-2086

Graduate School ETD Form 9
(Revised 12/07)

PURDUE UNIVERSITY
GRADUATE SCHOOL
Thesis/Dissertation Acceptance

This is to certify that the thesis/dissertation prepared

By Anurag Jain

Entitled Increasing Security Effectiveness in IT Enabled Products Using Balanced Scorecard Framework

For the degree of Master of Science

Is approved by the final examining committee:

James E. Goldman
Chair

Jeffrey L. Brewer

Lorenzo D. Martino

To the best of my knowledge and as understood by the student in the *Research Integrity and Copyright Disclaimer (Graduate School Form 20)*, this thesis/dissertation adheres to the provisions of Purdue University's "Policy on Integrity in Research" and the use of copyrighted material.

Approved by Major Professor(s): James E. Goldman

Approved by: Eugene H. Spafford 04/12/2010
Head of the Graduate Program Date

Graduate School Form 20
(Revised 1/10)

PURDUE UNIVERSITY
GRADUATE SCHOOL

Research Integrity and Copyright Disclaimer

Title of Thesis/Dissertation:
INCREASING SECURITY EFFECTIVENESS IN IT ENABLED PRODUCTS USING BALANCED SCORECARD FRAMEWORK

For the degree of MASTER OF SCIENCE

I certify that in the preparation of this thesis, I have observed the provisions of *Purdue University Teaching, Research, and Outreach Policy on Research Misconduct (VIII.3.1)*, October 1, 2008.*

Further, I certify that this work is free of plagiarism and all materials appearing in this thesis/dissertation have been properly quoted and attributed.

I certify that all copyrighted material incorporated into this thesis/dissertation is in compliance with the United States' copyright law and that I have received written permission from the copyright owners for my use of their work, which is beyond the scope of the law. I agree to indemnify and save harmless Purdue University from any and all claims that may be asserted or that may arise from any copyright violation.

ANURAG JAIN
Printed Name and Signature of Candidate

06/12/2010
Date (month/day/year)

*Located at http://www.purdue.edu/policies/pages/teach_res_outreach/viii_3_1.html

INCREASING SECURITY EFFECTIVENESS IN IT ENABLED PRODUCTS USING BALANCED SCORECARD FRAMEWORK

A Thesis

Submitted to the Faculty

of

Purdue University

by

Anurag Jain

In Partial Fulfillment of the

Requirements for the Degree

of

Master of Science

August 2010

Purdue University

West Lafayette, Indiana

To my family for their love, support and inspiration.

ACKNOWLEDGMENTS

To Prof. James E. Goldman, the author would like to express gratitude for being a role model and a great influence in developing the right mindset for information security. The author would like to thank Prof. Jeffrey L. Brewer for his valuable time and guidance and Prof. Lorenzo D. Martino for accommodating him and providing valuable feedback. The thesis committee has been very helpful and supportive. The author would also like to thank Dr. Melissa J. Dark for her important support and inputs.

The author would like to bring notice to two people who have mentored him to effectively deal with practical security issues and have been the inspiration for this study; Greg Handrick and Isaac Hopkins. The author would like to thank Dr. James L. Mohler for providing important guidance in carrying out this research.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABSTRACT

Jain, Anurag. M.S., Purdue University, August, 2010. Increasing Security Effectiveness in IT Enabled Products using Balanced Scorecard Framework. Major Professor: James E. Goldman.

IT enabled products are the result of a fusion of IT with the core functionalities of any product or device around us. This fusion is leading to numerous benefits and advantages that are just beginning to appear. However, with the increasing number and sophistication of vulnerabilities and threats in IT, the IT enabled products have also come in the line of fire. Due to the critical and diverse nature of these products, it is important that a holistic security framework exists that addresses security in the early phases of product development. The current state of security in IT enabled products strongly suggests this need along with the efforts of industry leaders in respective fields. In this thesis, the author has made an effort to address security in the IT enabled products by proposing a new framework based on the Balanced Scorecard. The proposed framework uses the concept of the four views and other characteristics of the Balanced Scorecard and it has a strong focus on security. The proposed framework has been evaluated by Prof. James E. Goldman; the chair of this thesis committee and its application has also been demonstrated to one of the discussed case examples of security failures. From this research, it has been concluded that the proposed framework can indeed effectively address security in the IT enabled products.

CHAPTER 1. INTRODUCTION

This chapter gives an overview of the thesis along with its scope and significance. The chapter provides the reader with relevant knowledge about the research area and establishes factors such as assumptions, limitations, delimitations and related definitions, followed by a short summary.

1.1. Background

The author has been fascinated by technology innovations and products since childhood. The author appreciates the tremendous capabilities of IT in today's world and feels excited about the future of IT. Being a technology enthusiast, the author sees great potential in IT and therefore, wants to be an active participant in its growth and development. Despite the manifold advantages, the IT segment is facing a challenge in the area of security and privacy. The fast pace of IT growth and the lagging pace of security development is widening the gap.

In this thesis, the author has made an effort to address security concerns in the field of IT enabled products. The author makes a distinction between traditional IT products and IT enabled products. Innovations are leading to increasing use of IT in diverse segments ("Nightly Business Report," 2009) and therefore, use of IT is no longer limited to traditional computer networks and software applications. Some of the examples of IT enabled products include modern medical devices, electronic banking systems, consumer IT devices, electronic voting machines, and process control systems to name a few. These products belong to different industry segments that rely on IT components for fulfilling and/or extending their functionalities.

Security vulnerabilities in IT are expected to rise ("Sophos Security Threat Report," 2009) and this poses a significant security challenge for IT enabled devices. Therefore, it is important that security concerns are given an equal priority so that these products do not get abused. In this thesis, the author has investigated the symptoms of the security problems in IT enabled products and proposed a framework-based solution that strongly focuses on security and business strategies. The author has used the Balanced Scorecard (Kaplan & Norton, 1992, 1993, 1996a, 1996b) as the basis for developing a new framework for addressing security in IT enabled products. The author prefers this framework because it is an easy workable solution, an industry standard and it has a strong focus on business strategy. The author believes that security can be addressed effectively when business strategy is taken into consideration.

1.2. Scope

IT security is a more mature discipline than security in IT enabled products. This is evident from the fact that there are well-defined frameworks and standards for IT security. Examples of these standards include ISO, NIST, FIPS and Common Criteria, to name a few. On the other hand, solitary efforts from leaders like Microsoft, Cisco, and Department of Justice, to name a few, address security concerns for a specific product or technology area, but a common security framework for IT enabled product family is missing. Security requirements vary in cases of IT enabled products because of their specific applications in diverse segments. For example, an implantable medical device might use wireless technology for communication purposes, but its core function is to provide medical support. On the other hand, a wireless access point might use the same wireless technology as an implantable medical device, but differences in associated security risks are apparent. Therefore, existing security standards may not prove to be effective for IT enabled products because the existing security standards focus on historically developed IT information systems/products and not on IT enabled products. Hence, it is important that the

horizon of security in IT products is widened to address security aspects of IT enabled products as well. The author prefers to use the term IT enabled products to include all products (traditional IT and IT enabled products) that rely on some form of IT functionality.

In the thesis, the author has tried to provide a common framework that is applicable to the family of IT enabled products. The proposed framework aims to increase security effectiveness in IT enabled products by focusing on business strategy and security requirements. Application of the framework has been illustrated with the help of an example that highlights the benefits and validity of the proposed solution. The effectiveness of the proposed framework has been measured on the basis of an evaluation by a subject matter expert.

1.3. Significance

IT enabled products have transformed our lives and are still in the process of evolution. According to the report from the Nightly Business Report in partnership with Knowledge@Wharton (“Nightly Business Report,” 2009), it can be seen that IT technology has the largest share in the top thirty innovations of the last thirty years. This innovation and growth in the field of IT is bound to startle us in the future as well. The family of IT enabled products is getting bigger and bigger with the increasing fusion of IT in different industry segments and verticals. Our lives are increasingly becoming dependent on various aspects of IT. Consequently, IT has also increased the risk rating of these products by introducing new vulnerabilities. The variety of attacks and malware are expected to rise in the future (“Sophos Security Threat Report,” 2009). The report also indicates that count of data leaks, identity thefts, and infected web pages is rapidly climbing. All these threats pose a significant security threat. It is therefore important to ask, is this reliance controlled, checked or verified? The answer is an unfortunate no.

The aim of this thesis is to address this question and provide a mechanism by which organizations can address security concerns with

confidence. The proposed framework, being generic in nature, gives organizations the freedom to integrate and/or develop other standards or frameworks that deal with a specific technology. The purpose of this framework is to allow organizations to evaluate their security posture based on the critical success factors and to align security with the business strategy.

1.4. Research Question

Can we increase security effectiveness in IT enabled products using Balanced Scorecard framework?

1.5. Assumptions

The following were the assumptions of this study:

1) An organization's cultural and environmental settings motivate and encourage efforts toward increasing security effectiveness.
2) The findings in the samples of security failures and risks discussed in the literature are consistent with other examples of security failures in IT enabled products.

1.6. Limitations

The following were the limitations of this study:

1) The proposed framework is based on a literature review and does not include any data collection from field or lab experiments for the purpose of the thesis.
2) Due to the limited time availability, the proposed framework cannot be applied to practical case(s) to measure its success.
3) The evaluation of the proposed framework has been carried out by a single subject matter expert.

1.7. Delimitations

The following were the delimitations of this study:

1) Only Balanced Scorecard was considered to propose the new framework; other frameworks were not analyzed.
2) Analysis of organizational cultural and environmental effects on security was beyond the scope of the study.
3) The focus of the proposed framework is limited to IT enabled products.
4) The proposed framework does not address the ethical and moral aspects of security.
5) The proposed framework is holistic in nature and therefore, applies to a wide variety of IT enabled products.

1.8. Definition of Key Terms

CSRF [Cross Site Request Forgery] – "is an attack which forces an end user to execute unwanted actions on a web application in which he/she is currently authenticated" ("Cross-Site Request Forgery - OWASP," 2010).

DNS Hijacking – "DNS hijacking or DNS redirection is the practice of redirecting the resolution of Domain Name System (DNS) names to rogue DNS servers, particularly for the practice of phishing, or to direct users to the ISP's own servers" ("DNS hijacking - Wikipedia, the free encyclopedia," 2010).

DoS [Denial of Service] – "attack is focused on making unavailable a resource (site, application, server) for the purpose it was designed" ("Denial of Service - OWASP," 2010).

DRM [Digital Rights Management] – "a system for protecting the copyrights of data circulated via the Internet or other digital media by enabling secure distribution and/or disabling illegal distribution of the data" ("What is DRM? – A Word Definition From the Webopedia Computer Dictionary," 2007).

EPROM [Erasable Programmable Read Only Memory] – “is a special type of memory that retains its contents until it is exposed to ultraviolet light. The ultraviolet light clears its contents, making it possible to reprogram the memory” (“What is EPROM? - A Word Definition From the Webopedia Computer Dictionary,” 1996).

Malware – “Short for malicious software, software designed specifically to damage or disrupt a system, such as a virus or a Trojan horse” (“What is malware? - A Word Definition From the Webopedia Computer Dictionary,” 2009).

Rootkit – “is a type of malicious software that is activated each time your system boots up. Rootkits are difficult to detect because they are activated before your system's Operating System has completely booted up. A rootkit often allows the installation of hidden files, processes, hidden user accounts, and more in the systems OS. Rootkits are able to intercept data from terminals, network connections, and the keyboard” (“What is rootkit? - A Word Definition From the Webopedia Computer Dictionary,” 2005).

Session Hijacking – “attack compromises the session token by stealing or predicting a valid session token to gain unauthorized access to the Web Server” (“Session hijacking attack - OWASP,” 2009).

Universal Plug N Play [UPnP] – “a networking architecture that provides compatibility among networking equipment, software and peripherals of the 400+ vendors that are part of the Universal Plug and Play Forum” (“What is UPnP? - A Word Definition From the Webopedia Computer Dictionary,” 2001).

WEP [Wired Equivalent Privacy] – “a security protocol for wireless local area networks (WLANs) defined in the 802.11b standard. WEP is designed to provide the same level of security as that of a wired LAN” (“What is WEP? - A Word Definition From the Webopedia Computer Dictionary,” 2004).

XSS [Cross-Site Scripting] – “attacks are a type of injection problem, in which malicious scripts are injected into the otherwise benign and trusted web

sites. Cross-site scripting (XSS) attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user" ("Cross-site Scripting - OWASP," 2010).

1.9. Chapter Summary

The chapter has provided insight to the motivation and need for this thesis. It has established the constraints and the factors under which the study was carried out. The chapter has also briefly highlighted the security concerns in IT enabled products and indicated a possible solution that aims to effectively address security in these products.

CHAPTER 2. LITERATURE REVIEW

The purpose of this chapter is to establish the need for a comprehensive security framework for IT enabled products, one that is closely tied with the business strategy of the organization.

Section one discusses security failures and risks in a variety of devices and industries. It attempts to illustrate the commonalities of security failures and risks and tries to establish the gap between the business strategy and security requirements of the IT enabled products

Section two covers the Balanced Scorecard and its derivatives. This section discusses the characteristics and adaptability of the Balanced Scorecard framework.

Section three gives a brief description of some of the security frameworks and standards prevalent among organizations. It highlights the emphasis of the frameworks and standards on involving security in early phases of IT product development.

Section four discusses key risk management and quality assurance methodologies.

Section five provides a conclusion to the literature review followed by the chapter summary. Each of the sub-section is devoted to the analysis of a single paper or work of the respective author(s) or researcher(s) and references made by them have been highlighted wherever required.

2.1. Examples of Security Failures and Risks in IT Enabled Products

This section will highlight security failures and risks associated with diverse industry segments. Even though the examples of IT enabled products

discussed in this section are totally distinct in nature, they exhibit a strong commonality in the root causes of security failures.

2.1.1. Security Analysis of Digital Rights Management

The music industry has been struggling against music piracy for years; Digital Rights Management (DRM) vendors and record label companies are fighting hard to provide adequate protection mechanisms that would prevent music from getting copied or transferred to discs and other media illegitimately. Halderman and Felten (n.d.) have provided a thorough security analysis in their paper on DRM for Sony-BMG compact discs (CDs). There are several causes of DRM problems; peer to peer networks, ripping applications, and a multitude of media player formats are a few. The different technologies and platforms add to compatibility challenges and security complexities.

In the case of CDs, discs are protected by either using built in security measures on the disc or some specialized DRM software to prevent music content copying or reproduction. These are termed as active or passive protection mechanisms respectively. In the paper, the analysis was carried out in various ways in order to subvert these measures in order to gain unauthorized access to the music on the discs.

The research group tested two DRM software (MediaMax and XCP) implemented by Sony-BMG in record labels. The research group performed attacks to bypass the passive and active protection mechanisms on the discs. They also showed that software used for active protection was vulnerable and could cause potential harm to the users' machines including privacy breach.

Passive protection relies on the identification of specific area on the disc to limit its use to audio players and prohibit use on computer drives. In the analysis, the research group demonstrated that it was possible to bypass this protection in the following ways (Halderman & Felten, n.d.):

1. Advanced software programs were tested that could easily bypass the protection area marked on the discs.
2. Platforms other than Windows allowed access to the music content readily on the marked discs.
3. By physically obscuring the protection area on the disc, CD drives could access the content (Reichert & Troitsch, 2002).

In case of active protection, the protection system on the disc installs the DRM software (MediaMax or XCP) on the users' machines. The software controls the number of times tracks can be ripped or burnt and on what media player devices they can be transferred and used. However, both MediaMax and XCP are vulnerable to attacks and can be easily compromised.

In case of XCP, it checks for blacklisted ripping applications to block access to the music on the discs. However, it is possible to either change the ripping application's process name or use new ones that are not yet blacklisted in order to provide access to the music. MediaMax, on the other hand is capable of installing itself even the when the user denies installation (Halderman, 2003; Halderman & Felten, n.d.). In the cases of both XCP and MediaMax, the DRM software is set to auto run to invoke installation once the disc is inserted into the drive.

The research group also illustrated that it was possible to bypass the watermark feature of MediaMax that was used to avoid ripping. It was possible to convert the music to an inferior file format without compromising much on quality. This revealed that the watermark used by MediaMax was weak.

MediaMax and XCP restrict the number of times that the tracks can be burnt. The DRM software keeps track of this information on a file stored on the computer. It was revealed that the mechanism could be bypassed by either using rollback attacks (state of machine was restored so that detection by the DRM software could be avoided) or modifying the file.

Another variety of attack involved deactivating the DRM software altogether in order to avoid any impact of the software on ripping, copying or transferring of music. In MediaMax, the deactivation was simple; stopping a software driver by issuing a single command was enough to deactivate it. In the case of XCP, the deactivation was difficult as it installs a rootkit to avoid detection (Russinovich, 2005b), but the research group proved that by changing the registry keys and following some steps it was possible to deactivate XCP as well.

The most dangerous aspects of both the DRM software (MediaMax and XCP) are the vulnerabilities they introduce to the users' machines. The following is a summary of findings (Halderman & Felten, n.d.):

1. It was possible to infect the users' machines by modifying the installed MediaMax code that got executed when the disk was read.
2. XCP used a rootkit to evade detection. The rootkit could be used by other malware, thus making users' machines vulnerable to attacks. XCP contacted the record label company (Sony) over the internet (Russinovich, 2005a). A similar behavior was observed with MediaMax that contacted the vendor to report the usage of media without users' knowledge leading to privacy breach.
3. The removal of MediaMax (Halderman & Felten, n.d.) and XCP (Nikki, 2005) required the users to visit a website that was found to lack security controls and could be used by an attacker to execute a malicious code on the users' machines.

The study is a valuable contribution in the field of digital rights management. It shows that not only does a poorly designed mechanism defeat the purpose of security; it can also compromise the security of the users, resulting in a double negative effect.

2.1.2. Security Analysis of Electronic Voting Machines

The electoral process is an important exercise as it decides the fate of a democratic nation. It is therefore considered a serious matter deserving of great care and high level security measures in order to preserve the integrity and faith in the electoral system. With the growing penetration of IT in all the dimensions of our lives, the electoral process is also seeing a change. In this paper presented by Feldman, Halderman and Felten (2006), security analysis of electronic voting machines highlights some stark revelations that can shatter the integrity and faith in the electoral process.

The research group conducted an in depth analysis of a Diebold voting machine AccuVote-TS. The research group tested the hardware and software security aspects of the voting machine to reveal its vulnerabilities.

The research group demonstrated that the votes registered against a particular candidate could be stolen and transferred to another candidate, while keeping the total vote count the same to avoid detection. This was possible with the help of malicious software installed on the voting machine. Although the records were encrypted, it was possible to compromise the encryption. It was also demonstrated that denial of service attacks could be launched on the voting machine to render it useless on the Election Day. This was made possible by installing a malicious code on the voting machine.

The research group has also referred to the security analysis conducted by Hursti (2006). Hursti (2006) suggested that if the attacker could gain physical access to the machine, she could easily install the malicious code by replacing the original EPROM chip with his chip containing the attack code. The attacker could also use the memory card to boot the machine in explorer mode where she could copy or run the malicious code or replace the original bootloader with a malicious one.

The research group also developed a specific virus to infect the voting machine and illustrated that the virus was capable of infecting several other machines through the reuse of memory cards.

There were three attacks conducted on the Diebold voting machine: installation of malicious software, denial of service attacks and installation of a virus. The attacks on the voting machines led to the following conclusions:

1. Malicious software can alter the results of a poll or cause denial of service attacks.
2. The memory card or EPROM chip of the voting machine can be changed quickly, thus allowing an attacker to compromise the integrity of the voting machine.
3. An infected voting machine with a virus can infect other machines via memory cards.

The paper shows the problems of improper design, lack of risk assessment and security management. A poorly designed architecture of voting machines might have altered the poll results or disrupt the election proceedings on a large scale.

2.1.3. Security Analysis of SOHO Routers

Heffner and Yap (n.d.) discuss security of popular SOHO (small office/home office) routers in this paper. The routers examined in the paper belong to some of the well known vendors like Linksys, D-Link, Belkin, and ActionTec. The vulnerabilities in these products are wide open with glaring loopholes. This paper attempts to reveal some of the findings in these routers.

The research revealed that all the routers are vulnerable to at least two or more attacks. The tested vulnerabilities belong to the following categories (Heffner & Yap, n.d.):

1. Cross Site Scripting Attacks (XSS).
2. DNS and Session Hijacking.
3. Default WEP key.

4. Cross Site Request Forgeries (CSRF).
5. Universal Plug N Play Attacks (UPnP).
6. Authentication Bypass.

Each of the four routers was tested for the above listed vulnerabilities using popular security penetration and vulnerability assessment tools. The successful exploitation of the vulnerability indicated that the particular product was vulnerable to the corresponding attack. Below is a table of security assessment results:

Table 2.1.

Security assessment results (Heffner & Yap, n.d.)

Vulnerability	ActionTec MI424-WR	Linksys WRT160N	D-Link DIR-615	Belkin F5D8233-4v3
Unauthenticated XSS	No	Yes	No	No
Authenticated XSS	No	No	Yes	No
DNS Hijacking	Yes	No	No	No
Session Hijacking	No	No	Yes	Yes
Default WEP	Yes	No	No	No
“Silent“ CSRF	No	No	Yes	Yes
Authentication Bypass	No	No	No	Yes
Local UPNP	Yes	Yes	Yes	Yes
CSRF UPNP	Yes	No	No	No

The results strongly suggest that the home routing products are vulnerable to easy attacks. The technology of the home routing products keeps changing at

a fast pace and therefore, the attacks or vulnerabilities listed above may not apply to newer products. However, the study indicates how little or no consideration is given to the security aspects during the design phase. It would be no surprise to find a number of vulnerabilities in the newer products from the same vendors.

2.1.4. Security Analysis of Implantable Medical Devices

Implantable medical devices (IMDs) have immensely helped patients to recover from medical aliments for which there was no solution in the past. These devices have saved several lives and are a great blessing of science to the humans. IMDs are the family of devices comprising of pacemakers, implantable cardioverter defibrillators (ICDs), etc. that use high end electronics to treat ailments related to the heart. However, these devices are also vulnerable to attacks. Halperin, et al. (n.d.) have demonstrated in the paper that it is possible to compromise information privacy on these devices. They also illustrated that it is also possible to change the configuration of these devices and cause them to malfunction.

The research group conducted two different attack types (passive and active) to test the security and privacy aspects of the IMDs. They used an ICD from a leading medical device manufacturer (Medtronics) for the purpose of analysis.

In the passive attack, the transmission between the ICD and the programmer was intercepted with the help of an oscilloscope. This attack revealed important information about the communication process that takes place between the two devices. This attack also revealed patients' personal and health information.

In the active attack, the researchers used the replay attacks to successfully change the configuration of the ICD. They could also cause the ICD to continuously emit information that may lead to power drainage. They demonstrated that with the use of active attacks, it was possible to change

patients' personal information on the ICD and to trigger shocks as well. Using specific electronic devices, software and reverse engineering it was possible to circumvent the security and privacy of ICDs. A potential area of security vulnerability may be related to ICD buffer overflows, protocol weakness, etc., and needs further analysis.

The research is limited to one single product of a particular manufacturer and therefore, the discussed vulnerabilities may not apply to other products across the industry. At the same time, it also indicates that other medical devices might be vulnerable as well. With the possibility of altering the device configuration and causing the devices to malfunction, it is apparent that the people using these devices are vulnerable to life threatening situations.

2.1.5. Security Vulnerabilities in Process Control Systems

In the white paper, Stamp, Dillinger, Young, and DePoy (2003) discuss the architecture for Process Control Systems with focus on security. Process Control Systems (PCS) or Supervisory control and data acquisition (SCADA) are the systems extensively used for supporting the public infrastructure service industries like electricity, water, petroleum, and manufacturing. With the increasing integration of PCS and IT services, PCS have become vulnerable to attacks. The reason for vulnerability is not only the integration of IT services, but also the increased exposure of PCS to the internet. The researchers have also discussed the need for security in PCS along with the common vulnerabilities found in PCS.

The PCS architecture can be described by the five essential components as under (Stamp, et al., 2005):

1. System Data: The System Data comprises of the process and control parameters specific to the PCS in consideration.

2. Security Administration: This is related to the security policies, operations, documentation, procedures, implementation, maintenance, and audit. In brief, this talks about the role of security in PCS.
3. Architecture: The architecture of PCS describes the hierarchy of control and data storage. It describes the working of PCS and its components.
4. Networks: The networks are the backbones that provide flow of control and data throughout the architecture of the PCS. These can be either the communication devices (modem, firewall, router, switch, etc.) or the link equipments (cables, microwave dishes, etc.).
5. Platforms: The platform includes the hardware and software applications that implement the functionality for control and data management.

The need for security in the PCS can be based on the following (Stamp, et al., 2005):

1. Critical infrastructure: PCS are comprised of highly critical public services like electricity, water, petroleum, etc., and therefore, it becomes important to stress security aspects. As automation is increasing with rapid increase in integration with IT, the exposure and vulnerabilities are scaling. The automation provides great benefits in terms of cost and performance but we need to address the security aspects as well.
2. Manufacturing: PCS has been used at a large scale in the manufacturing industry as well. Automation of processes based on high end microcontrollers has proved their worth in terms of efficiency, accuracy, and productivity. Again, security is one concern that should also be looked into to ensure safeguards against vulnerabilities.
3. Consequences: The vulnerabilities, if they materialize can seriously cause havoc in the PCS. The consequences can be any of the following:
    a. Physical impacts: Threats to life, property and/or environment.

b. Economic impacts: Compromise of operational integrity leading to economic loss.
c. Social impacts: Loss in consumer confidence and chances of social chaos.

Some of the common vulnerabilities that may be found in PCS are (Stamp, et al., 2005):

1. Classification of PCS Data: PCS data are not classified based on sensitivity levels. Unless the value of information is understood, no security mechanism can be effective. It is therefore important to establish the value of data.
2. Security Administration: To ensure that security plan is effectively rolled out, proper policies and procedures need to be established and followed in practice consistently. Auditing and security awareness are equally important to achieve the security objectives.
3. Architecture: The PCS architecture should be designed or restructured keeping security in focus. This ensures that the architecture itself is resilient to attacks.
4. Networks: The networks are perhaps the weakest links because new technologies like TCP/IP have been adopted on infrastructure that was inherently built to support proprietary or legacy protocols. Another important reason is the ill management of these new technologies that has resulted in the increased threat levels.
5. Platforms: Both proprietary/legacy and standard (Windows/Unix) platforms are vulnerable. PCS legacy platforms suffer from security vulnerabilities lacking essential features like strong authentication, password protection, etc. These platform vulnerabilities can be easily exploited when they are made accessible on the PCS networks. Similarly, modern platforms require a consistent focus on security (patch management).

The paper also discusses examples of recent security breaches in the PCS. These examples illustrate the gaps in the security implementation and lack of security in the PCS architecture. The cost of security breach especially in PCS can be enormous considering its critical nature and national significance.

2.1.6. Security Risks in E-Banking Systems

The Federal Financial Institutions Examination Council (FFIEC) in its article *E-banking – E-banking risks* (n.d.) has pointed out that transactional and operational activities in the e-banking systems pose significant security risks. It stresses that the risks should be addressed and mitigated for the benefit of the financial institutions/banks, other participating institutions and customers. It identifies and accepts that e-banking operations are vulnerable because of a lack of security standardization and increasing innovation.

To address this, FFIEC also suggests that appropriate policies, procedures and controls should be implemented by the banks/financial institutions. It stresses the importance of risk assessment, risk tolerance, and information security controls. It has addressed five risks associated to e-banking systems; these are the following ("E-banking – E-banking risks," n.d.):

1. Credit Risk: The risk is associated with the loans that are processed through online channels or e-banking systems. Credit risks include the following areas:

    a. Verification of customers' credentials.
    b. Identification of proxy agents for other participating institutions.
    c. Validity of loan information collected.
    d. Loan process monitoring.

2. Liquidity, Interest Rate, and Price/Market Risk: Increased exposure of the banking services through internet increases potential risks to the products

from consumers who want to exploit the service offerings in an illegitimate manner. This may require banks to change their policies to address the following concerns:

a. Reliance on brokered and/or rate sensitive deposits.
b. Reliability and integrity of the participating institutions.
c. Impact on growth due to increased market capability.
d. Fund volatility due to the risk of vulnerability exposure of the systems.

3. Compliance/Legal Risk: Due to evolving nature of e-banking systems, the legislation and compliance issues can be vague at times leading to misinterpretation. These issues are:

a. Geographic exposure attracts multiple regulations and compliances.
b. Legislation requirements for disclosure of information pertaining to transactions.
c. Documentation and record keeping.
d. Interpretation and validity of electronic agreements.

4. Strategic Risk: The e-banking systems clearly have the advantage of providing banks/financial institutions with an edge over competitors with the help of innovative products and services. On the other hand, e-banking systems also introduce new strategic risks. It is therefore necessary that the institutions should take notice of the following:

a. Monitoring the e-banking services through Management Information Systems.
b. Cost-benefit analysis of the e-banking systems.

c. Structural design of e-banking services to meet the customer needs.
d. Record keeping for evidence in the court of law.
e. Staffing requirements and cost for providing the e-banking services.
f. Management of e-banking systems from the support, procedural, and compliance standpoint.

5. Reputation Risk: It is important for banks/financial institutions to consider the value of its reputation and the risk associated with the e-banking systems. Materialization of any threat can seriously jeopardize its reputation and can cause tremendous damage. Some of these risks are:

    a. Loss in customer confidence.
    b. Confidential information leak.
    c. Service delivery failure.
    d. Service integrity, reliability, usability, and availability.

It should be noted here that e-banking risks can play an important role in dictating the business strategy of a given financial institution as these risks can directly impact its reputation.

2.2. The Balanced Scorecard Family

This section discusses the business Balanced Scorecard along with adoption of the scorecard approach for IT governance and IT security. The purpose of this section is to illustrate the adaptability of Balanced Scorecard in relation to assuring the security of the IT enabled products.

2.2.1. The Business Balanced Scorecard

Kaplan and Norton (1992, 1993, 1996a, 1996b) suggested a new framework to help organizations effectively realize their business vision and strategy. They coined it the Balanced Scorecard. The *Balanced Scorecard* (n.d.-a) article describes and highlights the important concepts of this approach. It states that the financial perspective in an organization is necessary but not the only important aspect. For organizations to realize their business goals successfully, view of customers, internal business processes, and learning and growth needs to be taken into account as well. Along with these perspectives, it is also necessary that organizations translate the business objectives into measureable targets and take the necessary initiatives to achieve them. Measurement and traceability of actions to business objectives are the key factors of success of the Balanced Scorecard approach. With time, Balanced Scorecard has become a widely used business standard and a popular and successful framework ("Balanced Scorecard Examples & Success Stories," n.d.). Some of the key benefits of using Balanced Scorecard are ("Balanced Scorecard," n.d.-a):

1. It helps organizations to understand their key performance indicators that drive businesses.
2. All the business units and individuals actively contribute towards the bigger objective of the organization by working towards their smaller targets.
3. Organizations can easily fragment the business objectives into workable and manageable pieces so that each business unit and individual understands what needs to be achieved and what their responsibility is.

The Balanced Scorecard emphasizes four important views of an organization that play key roles in identifying the critical success factors. These four different views ensure a comprehensive understanding of the overall

organizations mission and vision and therefore, enable organizations to set out the right objectives. These four perspectives are (“Balanced Scorecard,” n.d.-a):

1. Financial: This perspective makes sure that financial power is directed towards the right initiatives that will realize the business strategies.
2. Customer: It ensures that the business is meeting the expectations of their customers and that the customers are satisfied with the deliverables.
3. Internal Business Processes: They enable organizations to ensure that the objectives are met and provide feedback with the help of measurement metrics to address any gaps.
4. Learning and Growth: This perspective inculcates the culture of sharing, knowledge, and learning within the organizations. It is important for organizations to focus on learning and growth in today’s competitive environment.

Objectives are set out from each of these four views keeping the organization’s mission and vision in focus. Further, a set of measurement metrics are established to ascertain the benchmarks that can provide a scale for measuring success. A realizable set of targets corresponding to the measurement metrics are then established. This set of targets actually defines the benchmarks of success. Once the measurement metrics and targets are set, specific initiatives are laid out for the purpose of attainment. The traceability of actions to the business strategy is therefore connected through a chain of associations from initiatives to targets, targets to measurements, and measurements to objectives.

2.2.2. The IT Balanced Scorecard

Today’s businesses heavily rely on IT to achieve their business objectives. IT enables business to operate and grow with the help of various service and technology offerings. This has immensely increased the importance of IT in

businesses. The nature of IT is evolving dynamically at a rapid pace that has led to complexity in governance. This complexity leads to a lack of alignment and control over the IT functions and organizations often find problems in IT management. Hence, IT governance has become a major challenge for the organizations.

Gold (1992, 1994) and Willcocks (1995) suggested the IT Balanced Scorecard based on the concept of the original Balanced Scorecard framework (Kaplan & Norton, 1992, 1993, 1996a, 1996b). Additional research on the IT Balanced Scorecard was carried out by Grembergen and Bruggen (1997) and Grembergen and Timmerman (1998). In order to ensure that the IT governance is aligned with the overall business strategy, Grembergen (n.d.) has discussed how scorecards can be cascaded.

Grembergen defines IT governance as “The organizational capacity to control the formulation and implementation of IT strategy and guide to proper direction for the purpose of achieving competitive advantages for the corporation” (Grembergen, n.d., p. 2). In other words, IT governance is a vital function that provides an organization with the ability to effectively utilize the IT capabilities for the success of the organization. Because IT governance is closely related with the strategy of the organization; the inputs to IT governance can be linked with deliverables of the Business Balanced Scorecard. This feature of linking the IT governance with the Balanced Scorecard can be seen as a cascading effect.

The advantage of using Balanced Scorecard approach is that the IT Balanced Scorecard ensures traceability back to the business strategies and at the same time gives the management an opportunity to measure and manage IT functions. It is also essential that the initiatives follow a cause and effect relationship. The standard IT Balanced Scorecard comprises of four perspectives (Grembergen, n.d.):

1. User orientation: This perspective makes sure that IT contributes towards user needs.

2. Operational Excellence: It ensures that IT processes excel in providing services.
3. Future Orientation: It looks at the future needs of resources (both technical and human) required by IT in order to support the business functions.
4. Business Contribution: This perspective ensures that IT investments support the business needs and are justified in the eyes of the management.

The IT Balanced Scorecard can be further cascaded with the IT Development Balanced Scorecard and the IT Operational Balanced Scorecard. The IT Operational Balanced Scorecard is concerned with the infrastructure services that support the business functions for carrying out its operations and IT Development Balanced Scorecard is concerned with the development of new products and services to enable business growth and promotion.

Thus, by developing a strong focus on IT management using the Balanced Scorecard approach, organizations can effectively ensure IT governance for sustaining business operations and at the same time, they can also leverage their competitive advantage by using IT for business growth and development.

2.2.3. The Computer Security Balanced Scorecard

The dependence of businesses on IT invariably requires security for the protection of assets, services, infrastructure, and functions of IT. The problem in managing security is similar to managing IT; how can organizations measure security and ensure that security is aligned with the overall business strategy. DeLooze (2006) extended the Balanced Scorecard framework (Kaplan & Norton, 1992, 1993) for computer security.

The benefit of using Balanced Scorecard approach for computer or IT security is that the Balanced Scorecard for business, IT, and IT security can be cascaded for traceability (the ultimate advantage). Traceability ensures that the management can understand and appreciate the value of technology functions.

Traceability is necessary because IT and IT security are the support functions and do not contribute directly to the business revenue and therefore, it becomes crucial that investments in IT and IT security are justified. It is also important to ensure that the objectives of business, IT, and IT security are aligned with the overall strategy of the organization. Alignment ensures that the efforts of IT and IT security are directed towards achieving the business objectives of the organization. In other words, alignment ensures the direction (what needs to be done?) and traceability addresses the motivation (why it needs to be done?). If alignment and motivation are not given due importance, the basic aim of IT and IT security of supporting the business strategy cannot be fulfilled satisfactorily.

The other important benefits (as noted earlier) of using Balanced Scorecard approach are performance measurements and targets. The Computer Security Balanced Scorecard comprises four perspectives (DeLooze, 2006):

1. Users: These are the end users of the IT infrastructure and services.
2. Managers: They are the IT infrastructure and service owners concerned with the cost benefit analysis and return on investments.
3. System Administrators: They represent the administrators who run and manage the IT infrastructure and services.
4. Auditors: They are responsible for performing assessment of the IT infrastructure and services to evaluate the state of security.

These four perspectives ensure that security objectives take a balanced view of usability, cost, administration and quality. Security is a highly relative term and therefore, it is necessary to ascertain that security expectations are effectively met and justified. The aspects mentioned above ensure this by giving due importance to all the stakeholders and critical success factors. The business defines the high level plan of the organization and security strategies are deduced from the overall strategy, while keeping the four perspectives in focus.

This approach is similar to the cascading effect highlighted in the case of Business Balanced Scorecard and IT Balanced Scorecard.

Much like the Balanced Scorecard, each of the perspectives create objectives, set targets and performances metrics, and take necessary initiatives to contribute toward the goals of the IT or business strategy. The core advantage of Computer Security Balanced Scorecard is to provide organizations necessary confidence in the IT infrastructure and services from the security standpoint.

2.3. Security Frameworks

This section gives a brief overview of some of the prevalent security frameworks that attempt to align the security objectives with the business strategy. The frameworks also establish the importance of involving security in the early phases of product development. The findings from these frameworks substantiate the implementation aspects of the proposed framework.

2.3.1. Microsoft's Security Development Lifecycle

It is known ("SANS: The Top Cyber Security Risks," 2009) that Microsoft products are the biggest attack targets largely because of Microsoft's huge market share, well known vulnerabilities, and easily available exploits. As a result, Microsoft has taken initiatives to increase the level of security in their products.

Howard (2005) has discussed the Microsoft's Security Development Lifecycle (developed by Lipner, et al., 2005). The Security Development Lifecycle aims to address the security concerns in the software development lifecycle. The advantage of this framework is to involve security in the design phase itself rather than to apply it as a patch work later. In the article, Howard indicates that the Security Development Lifecycle has greatly reduced the number of defects by fifty to sixty percent, which is a notable improvement.

The important concepts of Security Development Lifecycle are (Howard, 2005):

1. Leadership and Education: Microsoft recognizes the need for an executive support for emphasis on security concerns. It realizes that without a proper executive support, an organization cannot effectively pursue the security ideology. Apart from leadership support, it also focuses on the culture of learning where people can gain knowledge and expertise in the field of secure designing and coding. Microsoft realizes that until and unless people learn about security there is no way they are going to build secure designs or codes.
2. Design Phase: The design phase is an important phase from the security standpoint. It is important that security is considered during the design phase as functional design requirements are set out in this phase. Functional requirements should cover security aspects of the application. Security features and implementations should be completed in the design specifications. It is necessary in this phase to include the impact of various components on security. Stress should be given to reduce the attack surface of the applications by disabling features that are not required.
3. Threat modeling: It is an integral part of the design phase. Threat modeling is necessary to ascertain the threats and vulnerabilities that will be introduced as a result of deploying the application. This helps to identify the vulnerabilities and to take necessary actions in order to mitigate the vulnerabilities. Threat modeling should be documented in the functional and design specifications as well.
4. Development Phase: In the development phase, tools along with guidelines and best practices for coding should be employed to ensure that code is implemented in a secure way. Microsoft has developed specific tools for this purpose. Secure coding is not only dependent on the

tools alone; developers also need to ensure that they understand the concepts of secure coding.

5. Security Testing: After the code is developed, the best way to check whether it has the necessary security features or not, is to perform a security assessment. The security assessment is based on fuzzing. Fuzzing provides a garbled input to the application and then verifies the application for errors. The assessment thus reveals the level of vulnerability in the application.
6. Starting a Security Push: Security push is a process where the documentation and code of the application are reviewed. This process ensures that the application follows what the architecture says. In other words, application conformance to the documentation is reviewed in order to track any changes during the development and investigate vulnerabilities that may have been left out.
7. Final Security Reviews: Final security review is a security checklist, which is performed by the central security team and the project team. It is a questionnaire about the security related to the components and the details about fuzzing. This review is done before the product is declared ready for shipment or release.
8. Security Response: Security response ensures that Microsoft learns from its mistakes and responds to vulnerabilities that are detected in the applications. Microsoft employs a dedicated staff to perform causal analysis of all the detected vulnerabilities. This is an important aspect of learning and works as a feedback mechanism to ensure that security concerns are quickly addressed.

2.3.2. Department of Justice's Systems Development Lifecycle

The Systems Development Lifecycle framework proposed by Department of Justice (DOJ) talks about a comprehensive approach to the planning, designing, development, operations, and management phase of information

systems. The framework has been discussed in great detail in *The Department of Justice – Systems Development Life Cycle Guidance Document* (2003).

The Systems Development Lifecycle framework gives importance to the planning phase in order to ascertain security and privacy requirements. DOJ realizes the significance of these two factors considering the vital roles they play in today's information systems. The planning phase requires risk assessment to identify the security and privacy impacts due to the proposed information systems. It also requires that the information systems are accredited to specific security standards and guidelines. The planning phase ensures that the high level risks have been identified and sets the right expectations with regard to security and privacy from the beginning of the system development. Once requirements are established, the design phase begins that translates the requirements into design solutions.

The Systems Development Lifecycle mandates that security testing must be performed once the system has been developed in order to ensure that the risks have been addressed and security gaps are identified. The testing also ensures whether the system complies with the stipulated security standards/certifications or not. The Systems Development Lifecycle gives a list of documents associated with different phases of the system development to ensure that security and privacy are addressed at the right places. These documents as proposed by DOJ include ("The Department of Justice – Systems Development Life Cycle Guidance Document," 2003):

1. Risk Management Plan.
2. System Security Plan.
3. Privacy Act Notice/Privacy Impact Assessment.
4. Security Risk Assessment.
5. IT Systems Security Certification & Accreditation.

2.3.3. Cisco's Integrated Security Architectural Framework

Cisco's *Integrated Security Architectural Framework Whitepaper* (n.d.) discusses how security can be effectively tied with the business requirements of an organization. The framework has been proposed and adopted by Cisco Global Government Solutions Group. The whitepaper presents a detailed framework that discusses requirement, implementation, and measurement aspects.

The article stresses on the importance of security involvement at the business level. The biggest advantage of this framework is to allow businesses to appreciate value in security, address security effectively, and understand risks. It also gives a brief description of the disadvantages when security is practiced in isolation. The catch is that isolated policy, risk, compliance, and business continuity management fall short of covering the entire security scope for any given organization. In other words, these pieces cover some aspects of security, but not all.

Cisco stresses the need for a comprehensive security approach that integrates all these pieces together with focus on business requirements. It also points out that though several security standards are available, they are not sufficient. It is likely that these standards fail to address all the security aspects of an organization and therefore, may leave gaps. The justification is that the security standards address only a segment of security with special focus on specific information assets/systems and therefore, may not address the varying needs of the different organizations.

The Integrated Security Architectural framework relies on the security requirements drawn from the business needs and proposes the use of multiple industry standards to address these requirements. Implementation should be followed by the measurement of outcomes to provide a feedback loop. On the other hand, compliance management can be ensured by identifying gaps in the outcomes and comparing them with the requirements of a specific

regulation/certification. This helps to verify the extent of requirements that have been addressed and identify the present gaps.

The Model as presented in the whitepaper (“Integrated Security Architectural Framework Whitepaper,” n.d.):

Define Requirements, Implement Requirements, and Measure Success

The requirement phase covers:

1. Framework: Specific industry security standard that provides the guidelines.
2. Policy: Specific security policy that aligns with business objective.
3. Standard: The means to implement the policy; security mechanisms.

The implementation phase covers:

1. Procedure: Detailed steps for implementing security.
2. Security Service: Identification of security service that will be addressed.
3. Project Name: The projects that will be addressed by the security services.

The measurement phase covers:

1. Risk ranking: Overall risk rating of the objective that security is addressing.
2. Delivery Scoring: Score for ascertaining the level of security achieved.

The measurements are divided into two levels: program/service level and problem identification metrics. The metrics are drawn from the business requirements using a balanced scorecard approach (“Balanced Scorecard,” n.d.-

b). The high level business metrics are translated into specific program or service level requirements that may include risk rating, CMM (Capability Maturity Model) or other similar delivery scores. These are further classified into lower tiered metrics or problem identification metrics that are related to specific parameters like uptime, SLA (Service Level Agreement), total spam blocked, etc. It stresses on the importance of defining metrics and suggests the use of text on security metrics by Jaquith (2007).

The balanced scorecard approach ensures that the management understands the state of security with the help of the lower tiered parameters. The security professionals, therefore, can easily show the management what measures are addressing which of the business risks.

2.4. Risk Management and Quality Assurance

The section will discuss some of the standardized and important methodologies on risk management and quality assurance of IT products.

2.4.1. NIST Special Publication 800-30

One of the key elements of security is to provide safeguards to assets based on the nature of risks associated with them. Therefore, it is essential that a proper risk management approach is adopted. Risk Management Guide for Information Technology Systems recommended by NIST ("NIST Special Publication 800-30," 2002) is one of the examples, which provides a comprehensive risk management methodology.

NIST Special Publication 800-30 identifies three key areas of risk management; these areas include "risk assessment, risk mitigation, and evaluation and assessment" ("NIST Special Publication 800-30," 2002, p. 4). Risk assessment is the first step in risk management and its function is to identify the vulnerabilities and threats that an asset faces. This is accompanied by assessment of controls that are or will be in place in the future. Thus, this

process helps in determination of nature of risks associated with an asset in a given environment. The objective of this step is basically to assign a risk rating to an asset and recommend ways to mitigate them. The output of this process is a risk management report.

Risk mitigation follows risk assessment and the objective of this step is to allow organizations an opportunity to reduce the identified risks to an acceptable level with the help of appropriate controls at a given cost. There are various strategies under risk mitigation that an organization can adopt; they can either accept the risks, use controls to mitigate them, transfer the risks, or eliminate the risks. The choice of strategy strongly depends on the management's outlook and risk appetite.

Risk evaluation and assessment is an ongoing process. It ensures that organizations remain informed about the current IT risk posture at all times. This step is essential to the risk management methodology because IT infrastructure of any given organization is dynamic in nature and the threats and vulnerabilities are subject to changes. Hence it becomes critical for an organization to keep itself updated with the current risks.

The NIST Special Publication 800-30 provides a sound methodology that allows an organization to focus its efforts and energies in the right direction and to the right degree in managing risks. The quantification of risk is a challenging task and investigation, deliberation and discussion are the keys to successful risk management methodology.

2.4.2. NIST Special Publication 800-36 and Common Criteria for IT Security Evaluation

Risk assessment provides an organization with the necessary information about the type of controls required for mitigating the risks. The next important step is the adoption and implementation of appropriate controls and mechanisms that address the identified risks. In the context of IT enabled products, this step can be related to rating the quality of products so that both the organizations as

well as consumers have faith in it. NIST Special Publication 800-36 provides the general guidelines that help organizations ensure quality of IT security products ("NIST Special Publication 800-36," 2003). However, the approach can be very well be adopted and used as guidelines by the organizations as a security checklist in verification of IT enabled product quality.

NIST Special Publication 800-36 stress on the importance of testing and evaluation of IT security products by programs like Common Criteria Evaluation and Validation Scheme (CCEVS), NIST Cryptographic Module Validation Program (CMVP), and other similar evaluation programs that are recognized internationally. The benefit of such an evaluation is that security product manufacturers gain knowledge of the quality level based on an unbiased assessment that helps them to further enhance the product quality. The other important aspects are that it gives the assessing body an opportunity to increase its learning and expertise and provides a fair rating mechanism of IT security products based on a neutral evaluation. The consumers are benefitted as well because evaluation certifications from a standard body can help them to make an informed and confident decision. The importance of an evaluation program is further augmented if it is backed by the government.

Common Criteria defines a specific methodology of assessing the quality of IT products ("Common Criteria for Information Technology Security Evaluation – Part 1," 2006). The assessment on broad terms aims to establish whether a given product provides the necessary security features to counter the threats or not. The assessment is based on the identification of assets and associated threats. This is followed by suggestive countermeasures that are considered appropriate for protection of assets from the identified threats.

Common Criteria distinguishes the conformance of the product to security objectives on the basis of features that are functional in nature and those which are operational in nature. Functional features are the features that are part of the product itself. Operational features are the ones related to actual usage of the product in a specific way under a given environment. Common Criteria highlights

this important distinction to ensure that the assessment of the product is focused on the functional IT features and not on non-IT features. Assessments are costly and the focus of Common Criteria is only on the product features.

Product evaluation is carried out in two steps. Step one determines the conditions of evaluation and establishes the functional and operational aspects. Step two is the actual evaluation process in which the functionalities of the products are tested. All the evaluations are carried out on the basis of a specific methodology. The result of evaluation indicates the conformity of product's security features with the stated security objectives.

In the context of IT enabled products, the author believes that due to sheer diversity in applications, such an approach may be difficult to implement. However, it cannot be ruled out that specific industries do not have any product certification authorities but at the same time, the increasing fusion of IT changes the scope and applicability of such certifications. It may be expected that in the future, respective certification authorities adapt to the changing scenario of this IT fusion and become better equipped with the challenges. In the meantime, organizations can proactively ensure quality assurance by drawing in expertise from various standards, guidelines, programs, practices etc. (example NIST, Common Criteria, etc.). At the same time organizations can also contribute towards industry wide learning through knowledge sharing and help in pooling efforts toward standardization.

2.5. Conclusion

The literature review along with the observations and critiques highlight the need for a holistic security approach to IT enabled product development. The examples discussed in the literature review highlight the following commonalities and the need for an integrated approach:

1. Lack of balanced view of stakeholders in defining requirements.

2. Lack of proper analysis and focus on security requirements during design phase lead to:
    a. Inadequate risk assessment.
    b. Poor focus on quality assurance.

The above conclusions are based on the fact that in all the examples of security failures, subverting the security mechanisms were easy and straight forward. The need for a holistic approach stems from the fact that if security is given priority, most of the vulnerabilities in the design phase can be easily avoided. Security experts can greatly aid in ensuring that the product has the necessary security features while keeping budget in focus. Another important benefit of involving security during the design phase is to understand the risks and have the opportunity to do work on them. Risk assessment is an important step in understanding the threat levels and it can greatly benefit in handling security concerns proactively. Stress on a disciplined security approach is evident from the risks and vulnerabilities discussed for Process Control Systems and E-Banking Systems. These examples illustrate the need for giving due importance to IT security for safeguarding the offered services in the respective areas. Further the need for an integrated approach of business and security is strengthened by the examples of security frameworks. In all the cases, respective organizations have focused on security involvement during the design phase and on nurturing security practices in line with the business needs. The frameworks also illustrate the need for a feedback mechanism based on testing and/or certification in order to establish the desired level of quality assurance. The literature review discussed some of the standardized approaches to risk management and quality assurance. In summary, the findings suggest that failures of not addressing security in the product development lifecycle via risk management lead to vulnerabilities and lack of systematic evaluations via quality controls leave the security gaps unaddressed.

Although, the discussed frameworks highlight the need for an integrated approach, a holistic framework that can be used in cases of IT enabled products is missing. The discussed frameworks pertain to specific industries or organizations that have developed them according to their needs and therefore, cannot be directly applied in cases of IT enabled products.

The intent of this literature review was to highlight the commonality of security failures across different industry segments and to emphasize on the need for a broader security scope for the family of IT enabled products. The benefit of 'one size fits all' approach is that the organizations can rely on one single framework to address security concerns with confidence irrespective of the technology.

2.6. Chapter Summary

Balanced Scorecard (Kaplan & Norton, 1992, 1993, 1996a, 1996b) gives the organization an opportunity to align their efforts with the business strategy with the help of the four perspectives. The aspects of measurement, target, initiative, and objective form the organization's toolkit to work towards their business strategy. The cascading of Balanced Scorecard ensures alignment and traceability back to the business strategy.

The examples of failures show strong similarities in the causes of security vulnerabilities and risks across various industry segments. These can be summarized as under along with the list of suggested tools that can be used to address the findings:

Table 2.6.

Findings and Proposed Tools

Findings	Proposed Tool(s)
Business strategy fails to take security into account as a basic requirement	Balanced Scorecard
Security failures can be avoided if the requirements are duly addressed at the right phases of product development	Balanced Scorecard
Risk assessment and risk mitigation are vital to security	NIST 800-30
Focus on quality is essential for product's success	NIST 800-36 and Common Criteria

The discussed frameworks highlight the importance of an integrated approach to security and stress on the involvement of security in the early phases of product development. The frameworks also indicate the significance of methodical approach to risk and quality management.

CHAPTER 3. METHODOLOGY

The chapter provides information on the research methodology that has been employed in the thesis for the development of the new framework. Section 3.2 and 3.3 discuss the research goals and the verification criteria respectively.

3.1. Research methodology

Case study has been employed as the research methodology in the thesis and it is one of the five types of qualitative analysis that employs data from multiple sources (Creswell, 1998). Creswell (1998) defines:

> A case study is an exploration of a "bounded system" or a case (or multiple cases) over time through detailed, in-depth data collection involving multiple sources of information rich in context. This bounded system is bounded by time and place, and it is the case being studied–a program, an event, an activity, or individuals. For example, several programs (multi-site study) or a single program (within-site study) might be selected for study. Multiple sources of information include observations, interviews, audio-visual material, and documents and reports. The context of the case involves situating the case within its setting, which may be a physical setting or the social, historical, and/or economic setting for the case (p. 61).

In this thesis, case study has been used for analyzing the different examples of security failures and risks. The sources of information are limited to

documents and reports (as presented in the literature review) and the thesis does not involve any other means of data collection methods.

The methodology used for developing the new framework for addressing information security in IT enabled products is based on three key areas. The first area is the identification of security failures and risks across varied examples of IT enabled products as presented in the literature review. The second is the development of the proposed framework based on the Balanced Scorecard and the third is the adoption of the standardized tools for risk management and quality assurance.

Case study has been employed in the phase one “Literature review” of the framework development lifecycle (figure 3.1). The findings of the discussed cases of security failures and risks have been summarized in the conclusion section of the literature review (section 2.5). These findings illustrate the need for a holistic security approach to IT enabled products. Further, this need has also been substantiated by the security frameworks discussed in the section 2.3 of literature review.

The phase one of the framework development lifecycle also covers the review of the Balanced Scorecard and its derivates along with NIST 800-53 and Common Criteria standards. The analysis of the Balanced Scorecard family (section 2.2) has highlighted the benefits and characteristics of the Balanced Scorecard framework, which have been used in the development of the proposed framework. Further, the NIST 800-53 and Common Criteria standards have been reviewed to cover the risk assessment and quality assurance aspects of security (section 2.4).

The phase two “Proposed Framework development” of the framework development lifecycle covers all the aspects of the proposed framework in detail. The last phase “Proposed Framework Application and Verification” covers the implementation and verification aspects of the proposed framework. The verification of the proposed framework is based on a checklist (section 3.3) and the implementation uses the case example of Diebold electronic voting machine.

The case of Diebold electronic voting machines has been discussed in detail in the section 2.1.2 of literature review. Premier Election Solutions, a subsidiary of Diebold, Inc. was the manufacturer of the electronic voting machines (Diebold, n.d.).

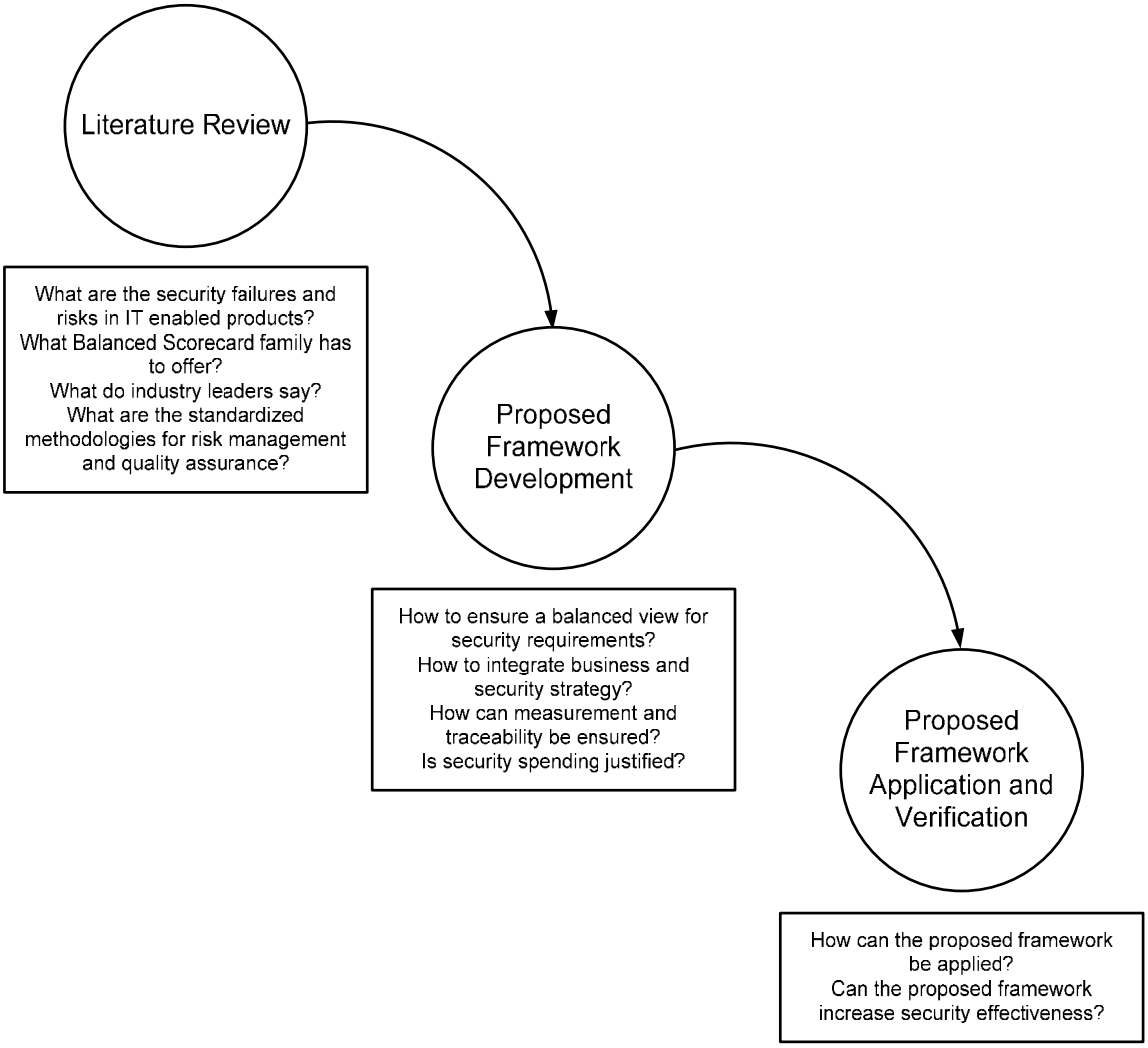

Figure 3.1. Framework development lifecycle.

3.2. Research goals

The analysis of security failures indicates the commonalities of security failures that substantiate the gap between the current and desired state of

security in IT enabled products. This gap can be addressed effectively by aligning the business strategy and security requirements of IT enabled products and using the adaptability and flexibility of the Balanced Scorecard framework.

The proposed framework intends to achieve the following goals:

1. Balanced view of the stakeholders for achieving security objectives.
2. Holistic security approach in the development of IT enabled products while keeping business strategies in focus.
3. Measurement of security objectives and traceability of actions back to the business strategy.
4. Ability for organizations to justify security spending.
5. Act as a meta-framework that allows use of other industry standards/methodologies/frameworks as plug-ins.

3.3. Verification criteria

The following checklist establishes the success criteria of the proposed framework. The checklist is based on the goals of the proposed framework illustrated above. The checklist intends to verify whether the proposed framework effectively addresses the findings or not. It also aims to validate that the discussed characteristics of the Balanced Scorecard framework have been successfully employed in the proposed framework.

Table 3.1.

Checklist for evaluating the success of proposed framework

Goals	Verification criteria	Check
Balanced view of the stakeholders for achieving security objectives	Does the proposed framework give due consideration to the involvement of important stakeholders?	Yes/No
	Does the proposed framework mandate the participation of security professionals and/or experts in the development of IT enabled products?	Yes/No
	Does the proposed framework help in establishing the security objectives on the basis of active involvement of all the stakeholders?	Yes/No
Holistic security approach in the development of IT enabled products while keeping business strategies in focus	Are the security objectives aligned with the business strategy of the organization?	Yes/No
	Do the security objectives give consideration to the critical success factors or key performance indicators of the organization?	Yes/No

Table 3.1 (continued).

Checklist for evaluating the success of proposed framework

	Does the proposed framework give importance to the risk assessment process during the design and/or development phase of IT enabled products?	Yes/No
	Does the proposed framework mandate the use of quality assurance mechanisms in IT enabled products?	Yes/No
Measurement of security objectives and traceability of actions back to the business strategy	Are the security initiatives tied back to the overall business strategy of the organization?	Yes/No
	Does the proposed framework provide scope for the measurement of security objectives?	Yes/No
Ability for organizations to justify security spending	Does the proposed framework allow scope for budgetary considerations?	Yes/No
	Does the proposed framework allow the management to monitor and exercise control over security spending?	Yes/No
Act as a meta-framework that allows use of other industry standards/methodologies/frameworks as plug-ins	Does the proposed framework provide high level security objectives?	Yes/No

Table 3.1 (continued).

Checklist for evaluating the success of proposed framework

	Is the proposed framework flexible to allow the use of other standards, guidelines, methodologies, and/or frameworks for achieving the security objectives?	Yes/No
	Is the use of standards such as NIST and Common Criteria suggestive in nature?	Yes/No

The above checklist has been developed by the author on the basis of the findings of the literature review (Chapter 2). In order to ensure that the above verification criteria measure what they are supposed to measure, face validity has been employed. Sekaran (2003) defines:

> Face validity is considered by some as a basic and a very minimum index of content validity. Face validity indicates that the items that are intended to measure a concept, do on the face of it look like they measure the concept (p. 206).

Under the given circumstances where actual implementation and results of the proposed framework cannot be measured, face validity was the only available option. The author had taken inputs from the chair of the thesis committee, Prof. James E. Goldman. He is a subject matter expert in Balanced Scorecard and information security among other disciplines. The checklist was reviewed and validated by him.

Because the measurement does not involve field data, the effectiveness of the proposed framework measured by the checklist alone may have introduced

some measurement errors. Unfortunately, these errors cannot be accurately ascertained until and unless the proposed framework is implemented in real life examples. The author has accepted these concerns along with the issue of validity as the limitations of the study.

The final evaluation of the checklist has been done by Prof. Goldman. The evaluation was carried out after the proposed framework was fully developed and its application was demonstrated. The results have been reported as percentage for each of the stated goals. The percentage was calculated by taking the ratio of the number of affirmative answers and the total number of criteria for each of the goals. The percentage calculated indicates the effectiveness of the proposed framework for each of the stated goals.

3.4. Chapter Summary

The chapter has provided insight into the research methodology employed in the thesis along with the research goals and verification process.

CHAPTER 4. THE PROPOSED FRAMEWORK

The chapter presents the proposed framework for addressing security in IT enabled products along with the justification of the four views, adapted from the Balanced Scorecard (Kaplan & Norton, 1992, 1993, 1996a, 1996b) and a complete description of the associated roles and responsibilities. It also provides a high level implementation and the application of the proposed framework with the help of the case analysis of Diebold electronic voting machine. The chapter concludes with the evaluation of the proposed framework's effectiveness.

4.1. The proposed framework for assuring security of IT enabled product development

The review of literature in the section 2.2.1 has provided insight into the characteristics of the Balanced Scorecard. The Balanced Scorecard relies on the concept of four views and objectives, measurements, targets and initiatives (Kaplan & Norton, 1992, 1993, 1996a, 1996b). Based on these characteristics of the Balanced Scorecard, the proposed security framework for IT enabled products also employs these concepts. The proposed framework is based on the lines of IT Balanced Scorecard (section 2.2.2) and Computer Security Balanced Scorecard (section 2.2.3) in terms of adapting the features of the Balanced Scorecard.

The four views ensure a balanced view in establishing the project strategies. The choice of the four views in the proposed framework has been discussed in the section 4.2. The project goals are established by the top management and therefore, the project strategies are aligned with the overall

mission and vision of the organization. The four views suggested in the framework are:

1. Project Manager: She is the project owner and also, the supreme project authority.
2. Project Teams: They represent the various teams that excel in different areas of project implementation.
3. Security Experts: They are security professionals who belong to various disciplines. They are responsible for the security and privacy aspects of the project. This team is also responsible for quality assurance and implementation.
4. Customers: These are the end users of the IT enabled products. They may also include users that implement the product for end use by another party.

The above description provides a simplified view of the proposed framework. The top management provides the high level business goals to the Project Manager. Project Teams and Security Experts work under the Project Manager's directives. The view 'Customers' may not be an actual group of people but it is a collection of various possible end users that will eventually use or implement the IT enabled product. This view ensures that throughout the development of the IT enabled product, the initiatives are strongly tied to the requirements of the end users and/or implementers. Though, it is possible that organizations may involve real people during the project development to better understand their requirements. This need will depend on the type of the IT enabled product and the targeted consumer base.

On a broad level, the high level objectives and the relation between the four views are shown in the figure below:

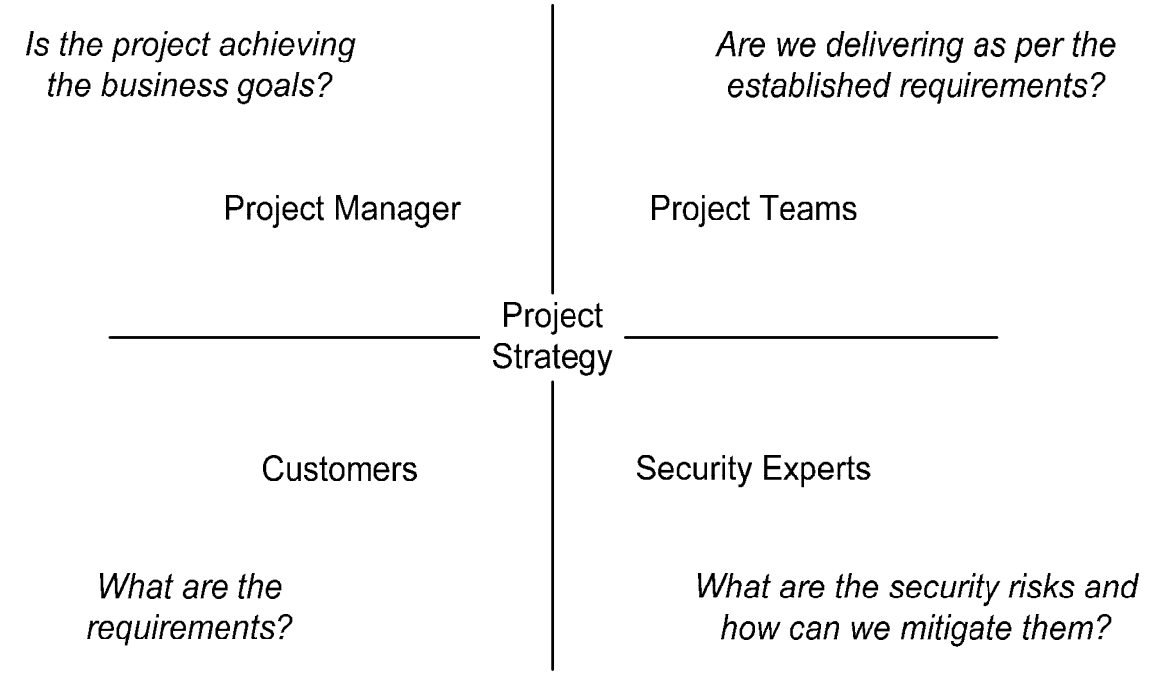

Figure 4.1. The proposed framework for IT enabled products.

The top management can also rely on the use of a framework such as the Balanced Scorecard. The business strategies from the Balanced Scorecard can serve as inputs to the proposed framework. The proposed framework can be integrated with the Balanced Scorecard in the following manner:

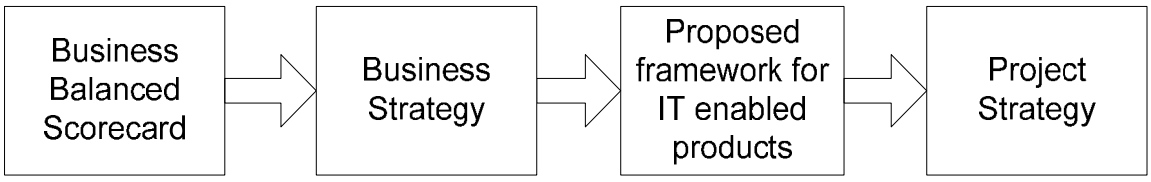

Figure 4.2. Cascading the Balanced Scorecard and the proposed framework.

The management can provide the high level strategies to the Project Manager. The Project Manager can work with the other three views to lay out the specific objectives, measurements, targets and initiatives to fulfill the stated objectives.

4.2. Justification of the four views

The conclusion (section 2.5) of the literature review highlights the need for the balanced view of stakeholders in defining the requirements and focus on security analysis in the design phase. In a given project, project head and project teams are the common stakeholders that are responsible for the project deliverables. The view of customers is important in the proposed framework because customers are the end users and therefore, they drive the requirements and eventually, dictate the success of any given project. The need for customers' view is further substantiated by the fact that Balanced Scorecard, IT Balanced Scorecard and Computer Security Balanced Scorecard (section 2.2) consider the view of the end users in the respective frameworks. Also, the concept of the balanced view in the proposed framework is based on the Balanced Scorecard and its associated benefits have been discussed in section 2.2.1.

The security experts in the project help in identifying the security concerns, implementing the necessary controls and providing assurance. The examples of security failures and risks (section 2.1) and the security frameworks (section 2.3) in the literature review have highlighted these requirements. Hence, it is imperative that the proposed framework considers security experts as one of the four views.

4.3. Description of responsibilities

The previous section started with a brief overview of the proposed framework. This section will provide the detailed responsibilities of the four views. The responsibilities have been discussed from the security standpoint and therefore, the discussion is not intended to be exhaustive for other responsibilities that may be associated in the project management lifecycle. The responsibilities of the four views are:

1. Project Manager: She is responsible for understanding the business objective of the project, establishing critical success factors and key

performance indicators, list of end users and/or customers, project budget, strategy, resources and timeline. The project manager acts as a key resource in translating the business objectives into successful deliverables. She is the ultimate project authority.

2. Project Teams: They perform the requirement analysis, develop SDLC or similar development lifecycles and propose design solutions on the basis of the high level security architecture developed by the security experts. The project teams need to strictly follow the guidelines as specified by the security experts and approved by the project manager. These guidelines may include but are not limited to the use of secure code libraries, software security and quality standards, or other practices/guidelines that the security experts consider important. The project teams also need to ensure that the design and functional changes are implemented only after they have been reviewed by the security experts and approved by the project manager. These changes may be required for feasibility and/or efficiency reasons. The key to successful and secure implementation is to ensure that the project teams work in unison with the security experts. The project teams may include but are not limited to the following group of implementers:

    a. Software application developers
    b. Administrators
    c. Hardware designers

3. Security Experts: The security experts may belong to different groups with expertise in various disciplines (industries/technologies) as per the nature and need of a given organization. For a given organization, the security experts may belong to sub groups such as security architects, audits, and operations. The sub groups are suggestive in nature and may be

expanded or collapsed as per the requirements of an organization. However, it is important to note here that security architects, operations and/or other groups concerned with the security implementation/design aspects should not be part of the audits group. This is necessary for avoiding conflicts of interest.

a. Security Architects: The responsibilities of the security architects include discussion on security risks, privacy, regulatory and compliance requirements. The architects furnish the risk model, risk assessment reports and risk mitigation strategies. On the basis of the preliminary analysis, they provide the high level security architecture that forms the basis for establishing the implementation guidelines for the project. They are also responsible for prescribing the use of specific standards, guidelines, and policies for a given project. The recommendations of the security architects need to be reviewed by all the project stakeholders and approved by the project manager.
b. Security Audits Group: The security audits group establishes the benchmarks for IT enabled product evaluation and may employ the use of standards for security and quality assurance. Product evaluation is an important activity that provides valuable feedback to all the project stakeholders. The security audits group may also perform routine evaluation to monitor the status and progress of the project. The scope of the audits needs to be defined by the project manager.
c. Security Operations Group: The security operations group provides necessary training, awareness and technical expertise to the project teams on security implementations, standards, guidelines, and policies. They may also be responsible for managing specific security functions of the project.

The figure below highlights the relation between the three security groups:

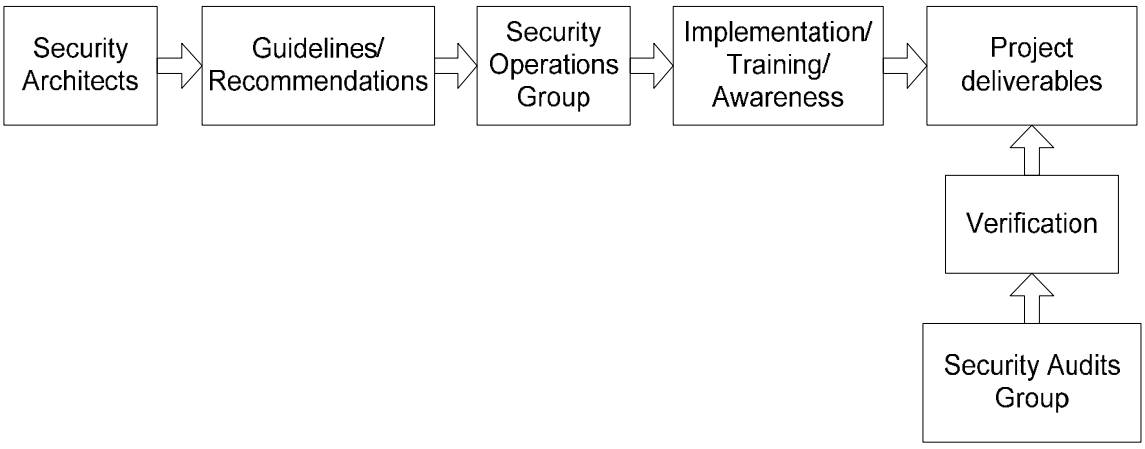

Figure 4.3. Relationships between security groups.

4. Customers: They represent the end users who will eventually use the product or implement it for third party customers. They may not represent an actual group of people but provide the necessary basis for driving the requirements of the IT enabled product development. An organization may employ various strategies to gather customer requirements when the IT enabled product is intended for commercial purposes and not for specific customer(s). In such a case, this view may be represented by a specific group of people belonging to the organization who are responsible for establishing the requirements.

The table below gives a brief description of the responsibilities of the four views discussed above:

Table 4.1.

Responsibilities of the four views

Views	Responsibilities
Project Manager	Project management
Project Teams	Project design and implementation

Table 4.1 (continued).

Responsibilities of the four views

Security Experts		
	Security Architects	Security analysis and recommendations
	Security Audits Group	Quality assurance and verification
	Security Operations Group	Security implementation and training
Customers		End use/implementation requirements of the IT enabled product

4.4. Implementation details

The section will describe the high level working and interaction of the various components of the proposed framework in the different project stages. The table below gives a suggested list of activities along with the stakeholders. The table describes the events in a chronological order. The implementation scenario primarily focuses on the security functions and processes in the development of IT enabled products. Details of functions specifically related to other views can be easily found in any of the established project management methodologies.

Table 4.2.

Implementation scenario of the proposed framework

Activity	Lead Actor(s)	Participating Actor(s)	Deliverables
Project kickoff	Management	Project Manager	High level details of project deliverables, budget, timeline, customers, critical success factors, and key performance indicators
Project startup meeting	Project Manager	Project Teams, Security Architects, Security Operations Group, Security Audits Group, Customers	Detailed analysis of critical success factors, key performance indicators, end users, project resources, and strategy
Preliminary requirement analysis	Project Teams, Security Architects, Customers	Project Manager, Security Operations Group	List of requirements/ deliverables
Initial security risk assessment	Security Architects	none	Risk assessment report, Risk mitigation plan
Risk acceptance	Security Architects	Project Manager	Approved risk mitigation plan
Security analysis	Security Architects	none	Security architecture, guidelines, standards, policies, compliance and regulatory requirements

Table 4.2 (continued).

Implementation scenario of the proposed framework

Security recommendations	Security Architects	Project Manager, Project Teams, Security Operations Group	Approved security architecture, guidelines, standards, and policies
Final requirement analysis	Project Teams, Security Architects	Project Manager, Security Audits Group, Customers	List of project deliverables in accordance with the approved security architecture
Security audit requirements	Project Manager	Security Audits Group	Scope and schedule of security audits
Discussion on security implementations	Security Architects	Security Operations Group	Detailed security implementation plan
Project development lifecycle	Project Teams, Security Operations Group	Project Manager, Security Architects, Security Audits Group	Approved project development lifecycle
Project implementation	Project Teams, Security Operations Group	none	Project deliverables
Iterative security audits	Security Audits Group	Project Teams, Security Operations Group	Audit reports (may be conducted on a routine basis)

Table 4.2 (continued).

Implementation scenario of the proposed framework

Learning and feedback	Security Audits Group	Project Manager, Project Teams, Security Architects, Security Operations Group	List of findings, suggested changes in the processes, implementations, and practices
Implementation of approved changes	Project Teams, Security Operations Group	none	Project deliverables
Final security risk assessment (when all changes are made)	Security Architects	Project Teams, Security Operations Group	Residual risk report
Residual risk acceptance	Security Architects	Project Manager	Approved risk posture (in case of any revisions, implementation is carried out by the Project Teams and Security Operations Group)
Final security audit	Security Audits Group	Project Teams, Security Operations Group	Final audit report

Table 4.2 (continued).

Implementation scenario of the proposed framework

Learning and feedback	Security Audits Group	Project Manager, Project Teams, Security Architects, Security Operations Group	List of findings for the entire project
Project submission	Project Manager	Management	Final project deliverables (if further improvements are not required)

The implementation scenario highlighted serves as an example to illustrate how the four views of the proposed framework will interact in a given environment. The objective of this illustration is to highlight how security aspects should be addressed in the development of IT enabled products. However, organizations can choose a specific project management methodology that suits the needs of a given project. The important thing to note here is the involvement of different Security Experts and the view of Customers during the different stages of the IT enabled product development.

The initial security risk assessment prior to the final requirement analysis is necessary to understand the environment in which the IT enabled product will be used and also, to establish the threat model. On the other hand, the security architecture is vital in ensuring that the accepted risk posture guides the development of the IT enabled products. Such an approach ensures that the security risks are understood and the development includes the necessary steps to mitigate them.

The list of activities may vary between various industries, verticals and organizations but the involvement of security in the early stages of development

needs to be reflected in the adopted project management methodology. Security Operations Group provides the necessary expertise, training and awareness to the Project Teams in the development of the IT enabled products. Once project implementation takes off, Security Audits Group plays an important role in providing valuable feedback to the project stakeholders. Security audit reports can highlight the weaknesses in security measures, process, practices and implementations. On the basis of the security audit reports, changes may be required as approved by the Project Manager.

When the project approaches completion, a final security risk assessment is required to identify the security gaps in the final product. The security risk assessment will provide a residual risk report that highlights these gaps. It is the responsibility of the project manager to either accept these risks or to suggest revisions for mitigation. Under such circumstances, it is reasonable to expect that the project manager may approach the top management for discussion and approval. Final security audit may be carried out for assessment of the project deliverables before submission. The audit findings can greatly assist in the learning process for the project stakeholders. Once the project manager feels that the final deliverables meet the business objectives, she can proceed with the submission.

An important thing to note here is that author has not used specific methodologies/standards/guidelines in the proposed framework other than employing the Balanced Scorecard framework. Depending on the maturity and expertise of an organization, it can either develop its own set of tools for carrying out the above mentioned activities or use the available ones. However, it is important that the scope and methodology of risk assessment and quality assurance tools are well defined. This is necessary because the effectiveness of security controls is strongly dependent on the nature of risk assessment and quality assurance tools adopted. As highlighted in the section 2.4, author suggests the use of NIST 800-30 for risk management and NIST 800-36 and

Common Criteria for quality assurance. Again, the standards may need to be modified as per the nature of the IT enabled product.

Figure 4.4 gives a pictorial description of the activities discussed in table 4.2. The figure highlights the flow and relationship between the various activities. Figure 4.5 shows the mapping between the objectives, measurements, targets, initiatives, and traceability (aspects of Balanced Scorecard) and the major activities of the proposed framework.

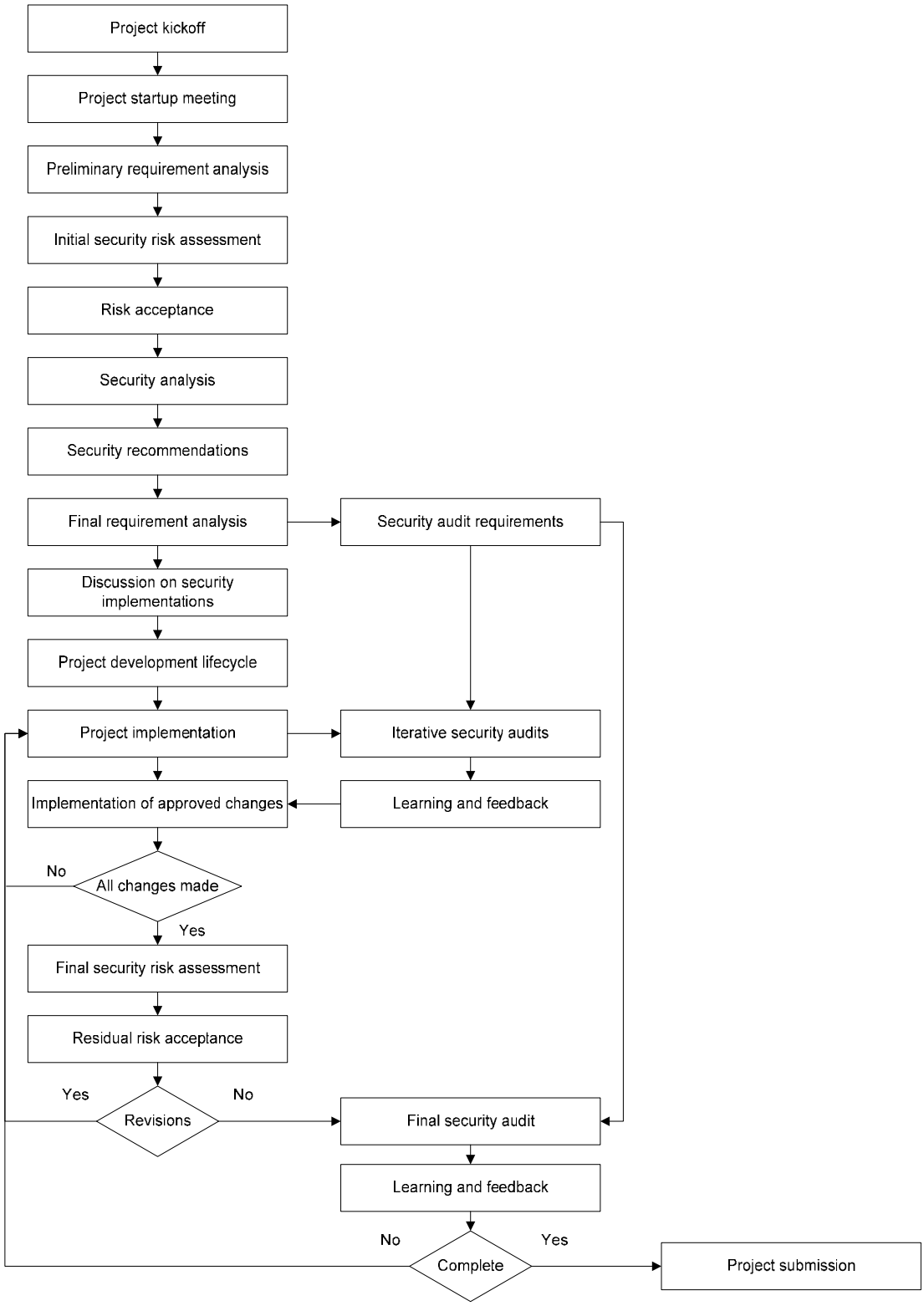

Figure 4.4. Flowchart of activities in the proposed framework.

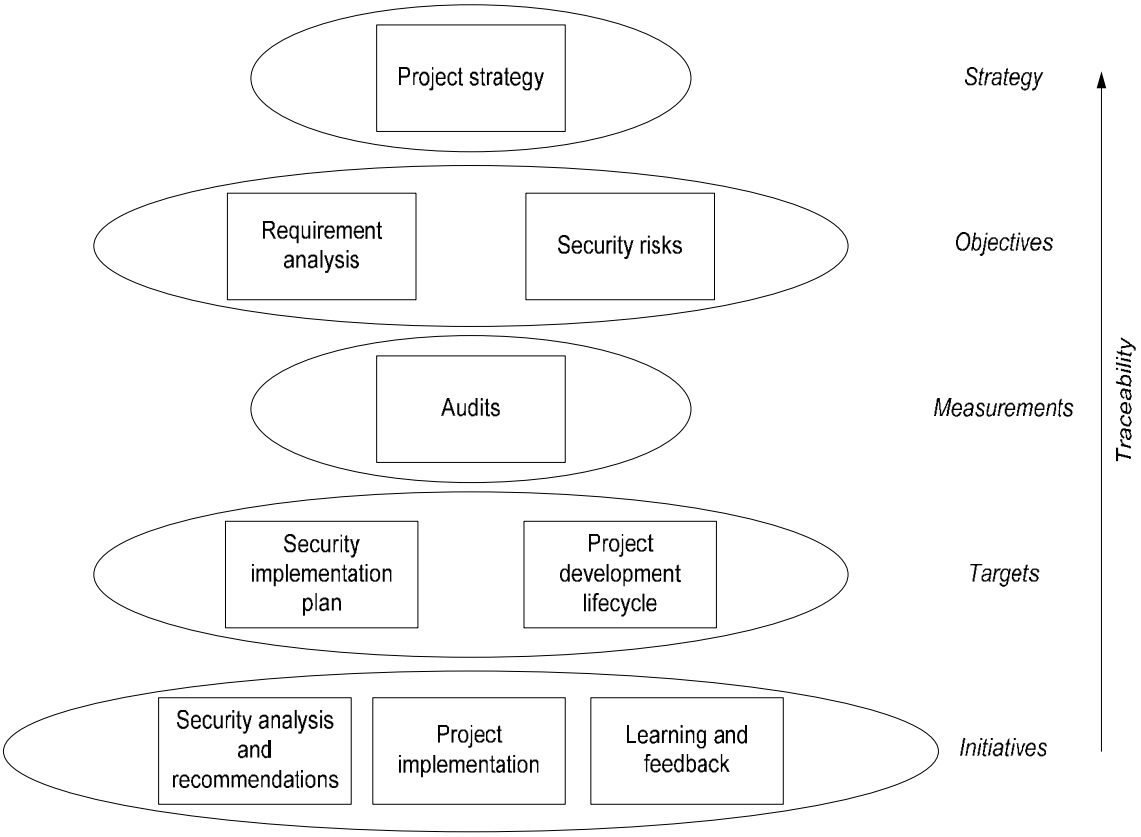

Figure 4.5. Mapping of the Balanced Scorecard aspects and activities of the proposed framework.

It is also necessary to understand the security aspects addressed by the proposed framework in order to appreciate its role in the secure development of IT enabled products. The table below describes the activities associated with the proposed framework that address the key security factors. The Lead Actor(s) and the Participating Actor(s) for the respective activities are the same as in table 4.2.

Table 4.3.

Key security factors addressed in the proposed framework

Activity	Deliverables	Key security factors addressed
Project kickoff	High level details of project deliverables, budget, timeline, customers, critical success factors, and key performance indicators	Identification of end users
Project startup meeting	Detailed analysis of critical success factors, key performance indicators, end users, project resources, and strategy	Identification of security resources and budget, detailed list of end users, and environment of product deployment/use
Preliminary requirement analysis	List of requirements/ deliverables	none
Initial security risk assessment	Risk assessment report, Risk mitigation plan	Identification of security risks, threat model, and security strategy
Risk acceptance	Approved risk mitigation plan	Establishment of risk posture
Security analysis	Security architecture, guidelines, standards, policies, compliance and regulatory requirements	Identification of high level security plan
Security recommendations	Approved security architecture, guidelines, standards, and policies	Establishment of high level security plan

Table 4.3 (continued).

Key security factors addressed in the proposed framework

Final requirement analysis	List of project deliverables in accordance with the approved security architecture	Identification of security controls
Security audit requirements	Scope and schedule of audits	Identification of security measurements
Discussion on security implementations	Detailed security implementation plan	Establishment of security implementation plan
Project development lifecycle	Approved project development lifecycle	Integration of security implementation plan with the project development lifecycle
Project implementation	Project deliverables	Implementation of security controls
Iterative security audits	Audit reports (may be conducted on a routine basis)	Audit(s) specific to validation of security measures
Learning and feedback	List of findings, suggested changes in the processes, implementations, and practices	List of security findings
Implementation of approved changes	Project deliverables	Implementation of revised security controls as per audit findings
Final security risk assessment	Residual risk report	Identification of residual risks in the final IT enabled product

Table 4.3 (continued).

Key security factors addressed in the proposed framework

Residual risk acceptance	Approved risk posture (in case of any revisions, implementation is carried out by the Project Teams and Security Operations Group)	Review of risk posture
Final security audit	Final audit report	Security audit of the final IT enabled product
Learning and feedback	List of findings for the entire project	List of security findings in the final IT enabled product
Project submission	Final project deliverables (if further improvements are not required)	Secure IT enabled product

4.5. Case analysis of Diebold electronic voting machine

The security analysis of Diebold electronic voting machine has been discussed in detail in section 2.1.2. Based on the analysis, the following vulnerabilities have been highlighted (p. 13):

1. Malicious software can alter the results of a poll or cause denial of service attacks.
2. The memory card or EPROM chip of the voting machine can be changed quickly, thus allowing an attacker to compromise the integrity of the voting machine.
3. An infected voting machine with a virus can infect other machines via memory cards.

It should also be noted that in the analysis, research work from Hursti (2006) has indicated the three possible ways in which the malicious code can be loaded in the voting machine. These were (p. 12):

1. By gaining physical access to the voting machine and replacing the original EPROM chip with an infected one.
2. By booting the voting machine in the explorer mode and copying/running the malicious code from the memory card.
3. By flashing the original bootloader with a malicious one using a memory card.

In order to implement the proposed framework with the help of this case example, the author has used the table 4.2 and table 4.3 described in the section 4.4. By using these tables, the author aims to prove that if during the design and development of the Diebold electronic voting machine, proposed framework was employed, the above mentioned security vulnerabilities would have been addressed.

In the following implementation example, all the four views along with the security sub groups have been considered (section 4.3). As per the definition of ‘Customers’ (section 4.1); the author has considered concerned government organization and voters under the view of ‘Customers’ because both the government organization (responsible for electoral process) and the voters are the end users of the voting machine.

The following table addresses the above mentioned security vulnerabilities in the Diebold electronic voting machine.

Table 4.3.

Case analysis of Diebold Electronic Voting Machine

Vulnerabilities	Activities addressing the vulnerabilities	Key security factors addressed	Specific initiatives (if any)
Installation of malicious software	Initial security risk assessment	Identification of security risks, threat model and security strategy	none
	Final requirement analysis	Identification of security controls	Code integrity check and strong authentication mechanisms for software upgrade/installation
	Project implementation	Implementation of security controls	none
	Iterative security audits	Audit(s) specific to validation of security measures	Check responses to installation of malicious code and verify the strength of authentication mechanisms
Easy access for replacing the EPROM/memory card or flashing the EPROM	Project startup meeting	Identification of end users and environment of product deployment/use	none

Table 4.3 (continued).

Case analysis of Diebold Electronic Voting Machine

	Initial security risk assessment	Identification of security risks, threat model and security strategy	none
	Final requirement analysis	Identification of security controls	Use of a physical lock, on-boot tamper checks, and authentication of EPROM and memory card
	Project implementation	Implementation of security controls	none
	Iterative security audits	Audit(s) specific to validation of security measures	Check responses to physical tamper to lock, EPROM, and memory card
Spread of infection via memory cards	Project startup meeting	Identification of end users and environment of product deployment/use	none
	Initial security risk assessment	Identification of security risks, threat model and security strategy	none

Table 4.3 (continued).

Case analysis of Diebold Electronic Voting Machine

	Security recommendations	Establishment of high level security plan	Memory card usage policy and standard operating procedure for verifying the integrity of machine, EPROM, and memory card
	Final requirement analysis	Identification of security controls	On-boot integrity check for code, EPROM, and memory card
	Project implementation	Implementation of security controls	none
	Iterative security audits	Audit(s) specific to validation of security measures	Check responses to infection and verify the standard operating procedure
Use of explorer mode to load the malicious bootloader	Initial security risk assessment	Identification of security risks, threat model, and security strategy	none
	Final requirement analysis	Identification of security controls	Strong authentication mechanisms for explorer mode
	Project implementation	Implementation of security controls	none

Table 4.3 (continued).

Case analysis of Diebold Electronic Voting Machine

	Iterative security audits	Audit(s) specific to validation of security measures	Verify the strength of authentication mechanisms

From the above table, it becomes clear that specific activities associated with the proposed framework address the security vulnerabilities identified in the case analysis of Diebold electronic voting machine and implement appropriate security controls to mitigate the risks. The traceability of security initiatives back to the business objective is ensured by the fact that security controls are part of the final requirement analysis and security controls are derived on the basis of the approved risk mitigation plan, both of which are chaired by the Project Manager. The targets are established on the basis of detailed security implementation plan and the project development lifecycle (figure 4.5). Security audits ensure that security controls are verified and targets are met and therefore, provide the important aspect of measurement. Hence, the proposed framework achieves the important aspects of Balanced Scorecard (Kaplan & Norton, 1992, 1993, 1996a, 1996b), which are objectives, measurements, targets and initiatives along with the balanced view of the stakeholders in IT enabled product development.

4.6. Measuring the success of the proposed framework

Based on the presentation of the proposed framework along with its implementation details and application to the case study of Diebold electronic voting machine, the chair of this thesis committee, Prof. James E. Goldman has evaluated the following scores. The scores for each of the stated goals (section 3.2) have been evaluated as per the established verification criteria (section 3.3).

Table 4.4.

Evaluation of the proposed framework

Goals	Verification criteria	Evaluation (Yes/No)
Balanced view of the stakeholders for achieving security objectives	Does the proposed framework give due consideration to the involvement of important stakeholders?	Yes
	Does the proposed framework mandate the participation of security professionals and/or experts in the development of IT enabled products?	Yes
	Does the proposed framework help in establishing the security objectives on the basis of active involvement of all the stakeholders?	Yes
Holistic security approach in the development of IT enabled products while keeping business strategies in focus	Are the security objectives aligned with the business strategy of the organization?	Yes
	Do the security objectives give consideration to the critical success factors or key performance indicators of the organization?	Yes
	Does the proposed framework give importance to the risk assessment process during the design and/or development phase of IT enabled products?	Yes

Table 4.4 (continued).

Evaluation of the proposed framework

	Does the proposed framework mandate the use of quality assurance mechanisms in IT enabled products?	Yes
Measurement of security objectives and traceability of actions back to the business strategy	Are the security initiatives tied back to the overall business strategy of the organization?	Yes
	Does the proposed framework provide scope for the measurement of security objectives?	Yes
Ability for organizations to justify security spending	Does the proposed framework allow scope for budgetary considerations?	Yes
	Does the proposed framework allow the management to monitor and exercise control over security spending?	Yes
Act as a meta-framework that allows use of other industry standards/methodologies/ frameworks as plug-ins	Does the proposed framework provide high level security objectives?	Yes
	Is the proposed framework flexible to allow the use of other standards, guidelines, methodologies, and/or frameworks for achieving the security objectives?	Yes
	Is the use of standards such as NIST and Common Criteria suggestive in nature?	Yes

The percentage effectiveness for each of the stated goals is as follows:

Table 4.5.

Effectiveness of the proposed framework

Goals	Score (Affirmatives/ No. of criteria)	Percentage Effectiveness
Balanced view of the stakeholders for achieving security objectives	3/3	100
Holistic security approach in the development of IT enabled products while keeping business strategies in focus	4/4	100
Measurement of security objectives and traceability of actions back to the business strategy	2/2	100
Ability for organizations to justify security spending	2/2	100
Act as a meta-framework that allows use of other industry standards/methodologies/frameworks as plug-ins	3/3	100

From the above evaluation, the author has established that it is possible to increase security effectiveness in IT enabled products using Balanced Scorecard framework.

4.7. Chapter Summary

The chapter has provided the detailed description of the proposed framework along with its implementation details and application. It has also provided evaluation of the proposed framework and thus, answered the research question.

CHAPTER 5. FINDINGS, CONCLUSIONS, AND RECOMMENDATIONS

The chapter provides the author's concluding remarks to the thesis by discussing findings of this study, conclusions, and future recommendations in the field of IT enabled product security.

5.1. Findings and Conclusions

The thesis has given an in-depth account of the proposed framework that aims to address the apparent lack of security in the IT enabled product development lifecycle. The essence of the proposed framework is strongly focused on security in the early phases of IT enabled product development. The author has based his research on the findings of the review of the literature (Chapter 2). The case examples of security failures and risks along with the security frameworks from industry leaders strongly indicate that security can be effectively addressed if it is involved during the IT enabled product development phase. The proposed framework ensures that security is addressed from the beginning of the product development lifecycle and that management can see value in security investments with the help of risk analysis based approach. The thesis has also hinted that instead of focusing on procedures, it is important to benefit from the approaches of the existing standards, guidelines, and frameworks to establish a matured security road map.

In the thesis, it has been shown that the Balanced Scorecard is a flexible and effective management framework and it can be effectively used in addressing security in IT enabled product development. The author has also stressed that risk assessment and quality assurance tools play an important role in addressing security concerns of the IT enabled products and they hold the key

to meaningful implementation of security controls. Apart from the evaluation mechanism employed in the thesis for measuring the effectiveness of the proposed framework, the discussed frameworks from industry leaders also emphasize the integration of security and business strategy.

The main contribution of this thesis to security in IT enabled products has been to highlight that the fusion of IT is changing the threat model for various products and therefore, it is important to recognize this change and analyze its security implications. The need for a comprehensive security framework also stems from the fact that IT is being increasingly used by industry segments that are not as matured as the mainstream IT organizations and therefore, the understanding of IT security is very much limited. Hence, the author has focused on the need and recognition for a holistic security approach in the IT enabled product development.

5.2. Recommendations

The proposed framework suffers from the limitation that its effectiveness cannot be measured from real data and therefore, the author suggests that the proposed framework is tested in real scenarios. The author also suggests that the proposed framework is tested in diverse cases of IT enabled products with various industry standards/frameworks serving as plug-ins. The author believes that the proposed framework provides organizations an opportunity to develop the right security mindset and hopes to see improvements in the current security standards in the IT enabled products.

5.3. Chapter Summary

The chapter has provided insight to the findings, conclusions, and recommendations for future work in the field of IT enabled product security.

LIST OF REFERENCES

LIST OF REFERENCES

Balanced Scorecard. (n.d.-a). Retrieved September 26, 2009, from http://www.12manage.com/methods_balancedscorecard.html

Balanced Scorecard. (n.d.-b). Retrieved September 28, 2009, from http://en.wikipedia.org/wiki/Balanced_scorecard

Balanced Scorecard Examples & Success Stories. (n.d.). Retrieved November 8, 2009, from http://www.balancedscorecard.org/BSCResources/ExamplesSuccessStories/tabid/57/Default.aspx

Common Criteria for Information Technology Security Evaluation - Part 1. (2006). Retrieved November 7, 2009, from http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R1.pdf

Creswell, J.W. (1998). *Qualitative inquiry and research design: Choosing among five traditions.* Thousand Oaks, CA: Sage Publications, Inc.

Cross-Site Request Forgery - OWASP. (2010). Retrieved March 6, 2010, from http://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)

Cross-site Scripting - OWASP. (2010). Retrieved March 6, 2010, from http://www.owasp.org/index.php/Cross-site_Scripting (XSS)

DeLooze, L. L. (2006). *Creating a Balanced Scorecard for Computer Security*. Retrieved September 26, 2009, from http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=1652071

Denial of Service - OWASP. (2010). Retrieved March 6, 2010, from http://www.owasp.org/index.php/Denial_of_Service

Diebold. (n.d.). Retrieved November 8, 2009, from http://en.wikipedia.org/wiki/Diebold

DNS hijacking - Wikipedia, the free encyclopedia. (2010). Retrieved April 16, 2010, from http://en.wikipedia.org/wiki/DNS_hijacking

E-Banking - E-Banking Risks. (n.d.). Retrieved September 29, 2009, from http://www.ffiec.gov/ffiecinfobase/booklets/e_banking/ebanking_01_risks.html

Feldman, A. J., Halderman, J. A., & Felten, E. W. (2006). *Security Analysis of the Diebold AccuVote-TS Voting Machine.* Retrieved October 4, 2009, from http://itpolicy.princeton.edu/voting/ts-paper.pdf

Grembergen, W. V. (n.d.). *The Balanced Scorecard and IT Governance*. Retrieved September 23, 2009, from http://www.itgi.org/ContentManagement/ContentDisplay.cfm?ContentID=33582

Grembergen, W. V. & Bruggen, R. V. (1997, October). *Measuring and improving corporate information technology through the balanced scorecard technique* (pp. 163-171). Proceedings of the Fourth European Conference on the Evaluation of Information Technology, Delft.

Grembergen, W. V. & Timmerman, D. (1998, May). *Monitoring the IT process through the balanced scorecard* (pp. 105-116). Proceedings of the 9th Information Resources Management (IRMA) International Conference, Boston, MA.

Gold, C. (1992). *Total quality management in information services - IS measures: a balancing act*. Boston, MA: Ernst & Young Center for Information Technology and Strategy.

Gold, C. (1994). *US measures - a balancing act*. Boston, MA: Ernst & Young Center for Business Innovation.

Halderman, J.A. (2003). *Analysis of the MediaMax CD3 copy-prevention system*. Technical Report TR-679-03, Princeton University Computer Science Department, Princeton.

Halderman, J. A., & Felten, E. W. (n.d.). *Lessons from the Sony CD DRM Episode*. Retrieved October 4, 2009, from http://www.cse.umich.edu/~jhalderm/pub/papers/rootkit-sec06.pdf

Halperin, D., Heydt-Benjamin, T. S., Ransford, B., Clark, S. S., Defend, B., Morgan, W., et al. (n.d.). *Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses*. Retrieved September 18, 2009, from http://www.secure-medicine.org/icd-study/icd-study.pdf

Heffner, C., & Yap, D. (n.d.). *Security Vulnerabilities in SOHO Routers.* Retrieved September 18, 2009, from http://www.sourcesec.com/Lab/soho_router_report.pdf

Howard, M. (2005). *How do they do it? A Look Inside the Security Development Lifecycle at Microsoft*. Retrieved September 9, 2009, from http://msdn.microsoft.com/en-us/magazine/cc163705.aspx

Hursti, H. (2006). *Diebold TSx evaluation: Critical security issues with Diebold TSx*. Retrieved October 4, 2009, from http://www.bbvdocs.org/reports/BBVreportIIunredacted.pdf

Integrated Security Architectural Framework Whitepaper. (n.d.). Retrieved September 28, 2009, from http://www.cisco.com/web/about/security/cspo/docs/IntegratedSecurityArchitecturalFrameworkWhitepaper.pdf

ISO - International Organization for Standardization. (n.d.). Retrieved December 3, 2009, from http://www.iso.org/iso/home.htm

Jaquith, A. (2007). *Security Metrics: Replacing fear, uncertainty, and doubt, 1st Ed*. Upper Saddle River, NJ: Addison-Wesley Professional.

Kaplan, R. S. & Norton, D. P. (1992, January-February). The balanced scorecard -Measures that Drive Performance*. Harvard Business Review,* 1992, January-February, 71-79.

Kaplan, R. S. & Norton, D. P. (1993, September-October). Putting the balanced score-card to work. *Harvard Business Review*, 1993, September-October, 134-142.

Kaplan, R. S., & Norton, D. P. (1996a). *The Balanced Scorecard – Translating Strategy into Action.* Boston, MA: Harvard Business School Press.

Kaplan, R. S. & Norton, D. P. (1996b, January-February). Using the balanced scorecard as a strategic management system. *Harvard Business Review*, 1996b, January-February, 75-85.

Lipner, S., Howard, M., et al. (2005). *The Trustworthy Computing Security Development Lifecycle*. Retrieved September 9, 2009, from http://msdn.microsoft.com/en-us/library/ms995349.aspx#sdl2_topic3

Nightly Business Report. (2009). Retrieved November 28, 2009, from http://www.pbs.org/nbr/site/features/special/top-30-innovations_home/

Nikki, M. (2005). *Muzzy's research about Sony's XCP DRM system*. Retrieved October 4, 2009, from http://hack.fi/~muzzy/sony-drm/

NIST Special Publication 800-30. (2002). Retrieved November 7, 2009, from http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

NIST Special Publication 800-36. (2003). Retrieved November 7, 2009, from http://csrc.nist.gov/publications/nistpubs/800-36/NIST-SP800-36.pdf

Reichert, V. K. & Troitsch, G. (2002). *Kopierschutz mit filzstift knacken*. As referenced by Halderman, J. A., & Felten, E. W. (n.d.). *Lessons from the Sony CD DRM Episode.*

Russinovich, M. (2005a). *More on Sony: Dangerous Decloaking Patch, EULAs and Phoning Home*. Retrieved from October 4, 2009, from http://blogs.technet.com/markrussinovich/archive/2005/11/04/more-on-sony-dangerous-decloaking-patch-eulas-and-phoning-home.aspx

Russinovich, M. (2005b). *Sony, Rootkits and Digital Rights Management Gone Too Far.* Retrieved October 4, 2009, from http://blogs.technet.com/markrussinovich/archive/2005/10/31/sony-rootkits-and-digital-rights-management-gone-too-far.aspx

SANS: The Top Cyber Security Risks. (2009). Retrieved November 14, 2009, from http://www.sans.org/top-cyber-security-risks/

Session hijacking attack - OWASP. (2009). Retrieved March 6, 2010, from http://www.owasp.org/index.php/Session_hijacking_attack

Sekaran, U. (2003). *Research Methods For Business: A Skill Building Approach, 4th edition.* Hoboken, NJ: John Wiley & Sons, Inc.

Sophos Security Threat Report. (2009). Retrieved November 28, 2009, from http://www.sophos.com/sophos/docs/eng/marketing_material/sophos-security-threat-report-jan-2009-na.pdf

Stamp, J., Dillinger, J., Young, W., & DePoy, J. (2003). *Common Vulnerabilities in Critical Infrastructure Systems*. Retrieved September 29, 2009, from http://www.sandia.gov/scada/documents/031172C.pdf

The Department of Justice - Systems Development Life Cycle Guidance Document. (2003). Retrieved September 9, 2009, from http://www.usdoj.gov/jmd/irm/lifecycle/table.htm

The FIPS Home Page. (n.d.). Retrieved December 3, 2009, from http://www.itl.nist.gov/fipspubs/

What is DRM? - A Word Definition From the Webopedia Computer Dictionary. (2007). Retrieved October 26, 2009, from http://www.webopedia.com/TERM/D/DRM.html

What is EPROM? - A Word Definition From the Webopedia Computer Dictionary. (1996). Retrieved April 16, 2010, from http://www.webopedia.com/TERM/E/EPROM.html

What is malware? - A Word Definition From the Webopedia Computer Dictionary. (2009). Retrieved April 16, 2010, from http://www.webopedia.com/TERM/m/malware.html

What is rootkit? - A Word Definition From the Webopedia Computer Dictionary. (2005). Retrieved April 16, 2010, from http://www.webopedia.com/TERM/r/rootkit.html

What is UPnP? - A Word Definition From the Webopedia Computer Dictionary. (2001). Retrieved April 16, 2010, from http://www.webopedia.com/TERM/U/UPnP.html

What is WEP? - A Word Definition From the Webopedia Computer Dictionary. (2004). Retrieved April 16, 2010, from http://www.webopedia.com/TERM/W/WEP.html

Willcocks, L. (1995). *Information Management. The evaluation of information systems investments*. London: Chapman & Hall.