The University of Pardubice

Faculty of Economics and Administration

Department of System Engineering and Informatics

Managing global cybersecurity implementation project using PMI methodology in a manufacturing company

Ruvimbo Jefrey

Master Thesis

2019

University of Pardubice
Faculty of Economics and Administration
Academic year: **2018/2019**

DISSERTATION ASSIGNMENT

(PROJECT, ART WORK, ART PERFORMANCE)

First name and surname:	**Ruvimbo Jefrey**
Study program:	**N6209 System Engineering and Informatics**
Identification number:	**E17922**
Specialization:	**Regional and Information Management**
Topic name:	**Managing global cyber security implementation project using PMI methodology in a manufacturing company**
Assigning department:	**Institute of System Engineering and Informatics**

Rules for elaboration:

The aim of the theses is to describe the implementation of a global security project using PMI methodology.

Outline:
- Introduction to cyber security
- Cyber security in manufacturing companies
- PMI Methodology in implementing cybersecurity
- Cyber security implementation in Foxconn (a manufacturing company)

Scope of graphic works:

Scope of work report
(scope of dissertation): **approx. 50 pages**

Form of dissertation elaboration: **printed/electronical**

Language of dissertation elaboration: **English**

List of specialized literature:

PROBST W. Christian, Matt BISHOP and Dieter GOLLMANN. Insider Threats in Cyber Security, Advances in Information Security. US: Springer, 2010. ISBN 9781441971333
CLARKE A. Richard and Robert KNAKE. Cyber War: The Next Threat to National Security and What to Do About It. US: HarperCollins, 2010. ISBN-10: 9780061962240
PROJECT Management Institution. Guide to the Project Management Body of Knowledge (PMBOK Guide). New York: PMI, 2017. ISBN 9781628251845

Tutor for dissertation: **Ing. Hana Kopáčková, Ph.D.**
Institute of System Engineering and Informatics

Date of dissertation assignment: **3 September 2018**

Date of dissertation submission: **30 April 2019**

L.S.

doc. Ing. Romana Provazníková, Ph.D.
Dean

doc. Ing. Pavel Petr, Ph.D.
Department Manager

In Pardubice, dated: 3 September 2018

DECLARATION

I declare that I have authored this thesis independently. All literary sources and information I have used in the thesis are listed in the References.

I have been acquainted with the fact that my thesis is subject to the rights and obligations arising from Act No. 121/2000 Coll., The Copyright Act, especially with the fact that the University of Pardubice has the right to conclude a license agreement for the use of this thesis as a School Work according to Section 60 (1) of the Copyright Act, and with the fact that if I should use this thesis or a license is granted to another entity, the University of Pardubice is entitled to request from me an adequate contribution to cover the costs incurred in creating the thesis, depending on the circumstances up to their actual amount.

I acknowledge that, in accordance with § 47b of Act No. 111/1998 Coll., On Higher Education Institutions and on Amendments to Other Acts (Higher Education Act), as amended, and with the Directive No. 9/2012 of the University of Pardubice, the thesis will be available to the public in the University Library and through the Digital Library of the University of Pardubice.

In Pardubice on April 30, 2019 Ruvimbo Jefrey

Acknowledgments

To start all with, I would like to thank the Almighty God for his goodness and mercies and the wisdom to compile all these and making it a great success. Again, I want to thank my Supervisor Mag. Hana Kopackova, for supporting, helping and recommendations in the process of writing this Master thesis. I want to thank my manager for helping me and making my dream come true, both at work and with this Master's thesis. I also would want to thank my team from Global cybersecurity implementation project in Foxconn. All your work and effort made this project a success and brought benefits to the company. Thank you Collet Muza, Vongai Nyahunzvi and Privillege Zhou for the wisdom and encouragement. I also want to thank special people in my life who always prayed and given me moral guidance throughout my studies My Parent Mr. and Mrs. Chimbambo; thank you for the undying encouragement toward this master's program.

Last but not least I would want to thank my husband Mr. Emmanuel Jefrey and My kids; Athalia

Jefrey and Malachi Jefrey, who endured painful and long time away from me during my studies,

Work, travels, and research. I can never pay back for the lost time. I love you all and God bless you.

ANNOTATION

Cybersecurity has been an important topic to most organizations in the 21st- century. Billions of dollars have been lost through cybersecurity and its threats. Various organization are tightening their security programs using various methodologies**.** The PMI approach focus on a well laid down plan by the Project Management Institude on implementing project within organizations**.** This study thus use the PM Methodology to implement cybersecurity in Foxconn a manufacturing company.

The main goal of this thesis is to identify the methods that are used to managing cybersecurity implementation project using PMI methodology in a manufacturing company. This has been achieved by conducting a semi-structured analysis of some of the methodologies that companies over the years have adopted in implementing their projects with much focus on the PM methodology.

KEYWORDS

Cybersecurity, PM Methodology, Project life cycle

ANOTACE

Kybernetická bezpečnost je pro většinu organizací v 21. století důležitým tématem. Miliardy dolarů byly ztraceny prostřednictvím kybernetické bezpečnosti a jejích hrozeb. Různé organizace zpřísňují své bezpečnostní programy pomocí různých metodik. Přístup PMI se zaměřuje na dobře stanovený plán k realizaci projektu v rámci organizací. Tato studie tak využívá metodiku PM k implementaci kybernetické bezpečnosti ve výrobní společnosti Foxconn.

Hlavním cílem této práce je identifikovat metody, které jsou využívány při řízení projektu implementace kybernetické bezpečnosti pomocí metodiky PMI ve výrobní společnosti. Toho bylo dosaženo provedením polostrukturované analýzy některých metodik, které společnosti v průběhu let přijaly při provádění svých projektů s velkým zaměřením na metodiku PM.

KLÍČOVÁ SLOVA

Kybernetická bezpečnost, Metodika PM, Životní cyklus projektu

CONTENTS

INTRODUCTION 11

1.1 The current state of global cybersecurity 13

1.2 Objectives 14

1.3 Significance of the study 14

1.4 Justification of the Study 15

1.5 Structure of the thesis 15

2. LITERATURE REVIEW 16

2.1 Defining Cybersecurity 16

2.2 Protecting Sensitive Data 17

2.3 The business Impact and Threats 17

2.4 Impacts beyond Data Loss 18

2.5 Manufacturing Environment and Cybersecurity 19

2.6 Creating Competitive Advantage through Cybersecurity 19

2.7 The Insider Threat 20

3. Cybersecurity in manufacturing Company. 22

3.1 Project Management Frameworks 22

3.1.1 Selecting Project Methodology 23

3.1.2 Best Project Methodology Practices 23

3.2 System Development Life Cycle (SDLC) Methodology 24

3.2.1 Waterfall model 25

3.2.2 Spiral Model 27

3.2.3 Iterative Incremental Model 27

3.2.4 The Agile Model 28

3.2.5 Extreme Programming (XP) Methodology 30

3.2.6 The Scrum Methodology 30

3.2.7 Dynamic Systems Development Methodology (DSDM) 31

3.2.8 Rapid Applications Development (RAD) Methodology 31
4. Project Management Using PMI Methodology 33
4.1 Defining PMI Methodology 33
4.2 Project Management Body of Knowledge 33
4.2.1 Five Project Management Process Groups: 34
4.2.2 Knowledge Areas of Project Management 34
4.3 The reason for choosing PMI methodology 34
4.4 General management Knowledge and skills 35
4.4.1 Application Area Knowledge, Standards and regulations 35
4.4.2 Cybersecurity Implementation application area: IT security 35
4.4.3 Cybersecurity application area: organization change 36
4.4.4 Understanding the project environment 36
4.5 Interpersonal skills 36
4.6 Project Life Cycle and Organization 37
4.6.1 Characteristics of Project Life cycle 38
4.6.2 Project Stakeholders 39
4.4.1 Project Global implementations of Cybersecurity project stakeholders 40
4.7 Organizational influences 41
4.7.1 Organization Structures 41
4.8 The initial Project Decision structure 43
4.9 Project Processes 43
4.9.1 Initiating Processes 44
4.9.2 Planning process group 45
4.9.3 Develop a project management plan 46
4.9.4 Collect requirements 46
4.9.5 Define scope and activities 47
4.9.6 Estimate activity resources and duration 47

4.10 Project activities Estimations 49
4.10.1 Risk management 50
5 CONCLUSIONS AND RECOMENDATIONS 55
5.1 RECOMMENDATIONS FOR FURTHER STUDIES 55
REFERENCES 57

LIST OF FIGURES

Figure 1: Phases of SDLC 24
Figure 2: The Waterfall Model 26
Figure 3: Phases of the spiral model 27
Figure 4: The iterative incremental model 28
Figure 5: The Agile Model 29
Figure 7: Monitoring and Controlling Process 37
Figure 8: The relationship between stakeholders and the project 40
Figure 9: Global Cybersecurity Project OBS 42
Figure 10: Overview of Project Management Process groups 44
Figure 11: Planning Process Group Processes 46

LIST OF TABLES

Table 1:Stakeholder's analysis for Foxconn cybersecurity project 45
Table 2: High level project plan 48
Table 3: Project Activity Estimation 49
Table 4: Human Resource Plan 50
Table 5: Overall risk and risk response 50
Table 6: Closing Process Group Checklist 53

LIST OF ABBREVIATIONS

BAU	Business as usual
BIS	Business Intelligence System
BIS	Business Information System
BPR	Business Process Re-Engineering
BPM	Business Process Modelling
FTE	Full time equivalent
ITU	International Telecommunication Union
PMI	Project management Institution
VPN	Virtual private network
WWW	World Wide Web

INTRODUCTION

Modern times can be characterized by increasing rates of change within every dimension of the environments in which we live. Global economic and political circumstances, technological infrastructure, and socio-cultural developments all contribute to an increasingly raging and dynamic environment for those who design and manage Information Systems (IS) for use in organizations, government, and other domains. Even weather patterns and events seem to change more rapidly in recent times. As our institutions (legal, political, economic, social, military) become increasingly global and interconnected, as we rely more and more on automated control systems to provide our needs for food, energy, and services, and as we establish Internet-based mechanisms for coordinating this global interaction, we introduce greater vulnerability to ourselves as individuals, for companies, and for our governments, including all other organizations. This increased dependence on cyberspace also inflates our vulnerability; isolation is no longer an option (Tirenin & Faatz, 1999). Perhaps no aspect of this phenomenon is as alarming and challenging as the need to understand the various risks to the security of the information systems of organizations and the methods for addressing those (Whitman & Mattord, 2004).

General Cyber and information security risks rising up (DHL, TNT losing business due to virus attack and its business unavailability) (Coburn, 2018). Customers of Foxconn increasing requirements in term of cyber and information security. There is no formal Cybersecurity policy and management in place within the community of Foxconn to address the issues. There was identified major change in the way the customer is looking on the risks protection supposed to be against targeted attack from the external or internal side of the network/factory vs formal protection targeted against accidental infection by malicious software and activity.

In order to address the customer requirements and prepare for further requests, general cybersecurity policies (CSP) need to be implemented

A Core team has been established to define the policy and basic requirements. Members of the team supposed to cover the actual customer requirements, further well known cyber and information security risks and technical knowledge to identify solutions to make sure the policy is followed as well as help to identify alternative approaches where necessary.

All business groups and Foxconn family companies connected to the same network need to prepare implementation plans, evaluate costs and risks and make sure they get comply within 2019.

This has raised the need to develop and implement cybersecurity measure using the PMI methodology. The threats and risks that have been the canker are from intentional human activity, and the world is now full of new, more sophisticated hackers, spies, terrorists, and criminal organizations that are dedicated to coordinated global attacks on our information assets in order to achieve their many goals. Some wish to inflict damage and loss for political reasons or for other selfish purposes, some are seeking "trade secrets" and proprietary corporate information, and others are seeking financial information with which to conduct fraud, identity theft, and other criminal acts. Another category of risks has arisen from new classes of increasingly-devious and effective malware capable of penetrating even the most recent perimeter defenses. These include not only viruses, worms, and trojans, but now also rootkits, distributed botnet attacks, and a new scary sophisticated category called the "Storm" class of malware, which includes programs which are self-propagating, coordinated, reusable, and self-defending peer-to-peer tools that use decentralized command and control and seem to use intelligence to dynamically defend themselves from users and software. Perhaps the greatest threat of all is the insider threat: the organizational member who is a "trusted agent" inside the firewall. This employee or another constituent with a valid username and password regularly interacts with the information assets of the organization and can initiate great harm to the confidentiality, integrity, or availability of the information system through deliberate activities. These and many other causes of threat to organization IS has posed a greater risk to all organizations causing organizations and institutions to spend much investment of protecting their systems. The need to develop and implement proactive measures to battle these attacks has become very necessary.

Developing and testing creative solutions and managerial strategies to identify these threats, analyze them, defend against them, and also to recover, repair, and control the damage caused by them is a critical management imperative(Kenneth, 2008). Leaders in government and industry must actively and aggressively support the ongoing design and implementation of effective, appropriate solutions that can be targeted to these diverse threats to their information assets and to the smooth functions of individuals, teams, organizations, and societies in the global network of systems.

We need to continually seek new and better solutions because the enemy is constantly improving the attack vectors. The alternative is not acceptable. The costs are too high. We must prevail.

1.1 The current state of global cybersecurity

As already mentioned above cybersecurity is a difficult task for both private and public organizations. Moreover, the defense capability of cyber users typically falls behind that of dangerous hackers who are quick to exploit holes, weaknesses, flaws, and vulnerabilities in hardware and software systems (Kemmerer, 2003). Rising expenses of computer hacking incidences progressively puts security of computer networks systems in danger. Failures in securing organization systems are partially rooted in the software vulnerability problem(Kemmerer, 2003: Knapp et al., 2009).

Most worrisome is that recent evidence which suggests that (77%) of private and public companies are operating with limited cybersecurity Most worrisome is that recent evidence which suggests that (77%) of private and public companies are operating with limited cybersecurity (Kessel, 2018). Unfortunately most organizations might not even have a clear picture of how, what, and where their most valuable information have adequate security.. The organization should first identify the key data and intellectual property then survey the cybersecurity abilities, get to the board forms, and different resistances, lastly update the shield that ensures the organization is protected (Kessel, 2018).

Questions that organizations must consider according to the report by EY Global Information Security Survey 2018–19:

- What are our most significant data resources?
- Where are our most clear cybersecurity shortcomings?
- What are the dangers we are confronting?
- Who are the possible threats to company cybersecurity?
- Have we previously been cyber attacked or compromised?
- How does our protection compare with our competition?
- What are our administrative duties, and do we consent to them?

According to Kessel (2018), over 50% of companies' protection of data is not integrated into strategy and execution plans. Surprisingly, according to the Global Information Security Survey 2018, bigger companies are most likely to be at risk than smaller companies. (58% versus 42%) (Kessel, 2018).

- **What is most important?**

It's nothing surprising that client data, monetary data and vital plans make up the main three most significant data that organizations might want to ensure (Kessel, 2018).

- **What are the greatest dangers?**

Research has established that susccessful cyber-attacks typically start as “phishing and/or malware’’ as entry points (Kemmerer, 2003: Knapp et al., 2009). Assaults concentrated on disturbance rank in third spot on the rundown, trailed by assaults with attention on taking cash (Kessel, 2018). According to the EY Global Information Security Survey 2018, despite the fact that there has been a considerable amount of discourse about insider dangers and state-supported assaults, the dread for inner assaults appears as number eight on the rundown; undercover work positions base of the rundown (Kessel, 2018).

One emerging issue that makes organizations more prone to these attacks is the measures and methodologies that organizations used when implementing these security systems. The need for a complex and well-structured methodology for implementing cybersecurity measures has thus become very crucial for the success of these security measures implementation. This thesis will focus on managing a global cybersecurity implementation project using PMI methodology.

1.2 Objectives

The objectives of this project will thus to enable organizations and institutions to know and focus on how well to implement cybersecurity measures using the PMI methodology. The specific objectives, however, are listed below:

- Discuss some current trends of cybersecurity
- Identify and elaborate on some cybersecurity measures in manufacturing companies ;
- Discuss some methodologies with emphasis on the PMI methodology used for cybersecurity implementation projects.
- Use the PMI Methodology for implementing cybersecurity in Foxconn (A manufacturing company).

1.3 Significance of the study

The study is important because it will not only propose and suggests the PMI methodology as a better approach of ensuring global cyber safety but also Cybersecurity is now considered as an important part of individuals and families, as well as organizations, governments, educational institutions, and business. It for new and upcoming organizations to learn from the falls of already existing companies who have been victims of cybersecurity frauds. The rapid expansion of technologies is also creating and making cybersecurity more challenging as we do not present permanent solutions for concerned problem. Although, organizations and

cyber institutions are actively fighting and presenting various frameworks or technologies to protect their network and information but all of these providing protection for short term only. However, better security understanding and appropriate strategies can help us to protect intellectual property and trade secrets and reduce financial and reputation loss.

1.4 Justification of the Study

A great deal of computer security involves deciding how we should protect information, resources, and assets. Folk theorems and slogans often emphasize the risk in neglecting any defense; e.g., “security is only as strong as the weakest link” and “there is no such thing as partial security.” Unfortunately, we can’t possibly do everything. Defensive measures generally involve a cost in time, money, or effort, so defending everything against all possible attacks is neither possible nor appropriate. This leaves us with hard decisions. Which measures should we choose and which methodology should be adopted in implementing the chosen measure? The success of the measure highly depends on how well it is implemented.

1.5 Structure of the thesis

This well-structured work is based on point by point analysis of the PMI methodology of implementing cybersecurity project in a manufacturing company. With this idea, this project work is divided into five parts.

Chapter 1 serves as an introduction to the thesis and presents the background to the study. It also provides the aims and objectives as well as a justification for the study.

Chapter 2 presents the review of literature on the threats and other methodology that has caused the organization to lose huge sums of monies to cyber fraud. The chapter helps to identify the gap to be filled by organization in the recent era since more threats are cropping each day.

Chapter 3 discusses methodologies adopted in the past and their success and failure rates and provides a justification for the method adopted for implementing cybersecurity.

Chapter 4 Provides a well-structured detailed of how the chosen methodology (PMI) can help achieve a successful project in global cybersecurity implementation.

Chapter 5 summarizes and concludes the study by making conclusions and recommendations based on the outcome of the methodology proposed.

2. LITERATURE REVIEW

There is significant academic literature that has viewed the term ‘’cybersecurity’’ from a particular perspective (Chang, 2012; Graigen et al, 2014). Based on the literature review described in various articles (Chang, 2012; Graigen et al 2014), it can be discovered that the term is utilized comprehensively and its definitions are profoundly factor, setting bound, regularly abstract, and, on occasion, uninformative. . There is a scarcity of literature on what the term really means and how it is defined inside different settings. The absence of a compact and comprehensively adequate definition that catches the multidimensionality of cybersecurity conceivably obstructs mechanical and logical advances. A considerable number of insightful work that exhibits the moves identified with organizational, financial, social, political, and other human dimensions that are inextricably tied to cybersecurity efforts has been proposed (Goodall et al., 2009). As quoted by Fredrick Chang, former Director of Research at the National Security Agency in the United States discusses the interdisciplinary nature of cybersecurity: *“A science of cybersecurity offers many opportunities for advances based on a multidisciplinary approach, because, after all, cybersecurity is fundamentally about an adversarial engagement. Humans must defend machines that are attacked by other humans using machines. So, in addition to the critical traditional fields of computer science, electrical engineering, and mathematics, perspectives from other fields are needed”*(Chang, 2012).

2.1 Defining Cybersecurity

We can thus adopt for the purposes of our study the definition of cybersecurity by International Telecommunication Union (ITU) as “Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets”(ITU, 2009). This definition explains our main goal of implementing global cybersecurity in a manufacturing organization.

2.2 Protecting Sensitive Data

To operate its day-to-day business successfully, a company must be adept at collecting, storing, processing, and transforming data. These capabilities allow a company to efficiently bill customers, create new products and services, and analyze sales trends to devise targeted marketing plans. This basic data ought to be secured like some other important resource (Wong 2004, Solms & Solms 2006). As the world has turned out to be increasingly dependedent on innovation, cutting edge crooks have likewise adjusted winding-up increasingly advanced and organized. (Wong, 2004: Cadieux, 2007: Harris et al., 2014). They can exploitr human blunder and weak security controls to take exchange privileged insights, installment card information, worker and client data, and other individual data. hackers loot organization information. Hackers do not only rob a company of their data but they also breach its trust with customer which in turn damages their reputation (Cadieux, 2007: Harris et al., 2014). Think what could possibly happen in the event that somebody messages a decoded unencrypted file to the wrong recipient. Also, the company may lake the technology innovation and process that helps to distinguish and control high hazard information through association or throughout the organization. Wong (2004) noted awareness of data fraud and individual security has never been higher, and workers and clients anticipate that your organization should ensure their delicate data. The government, administtrators and numerous industry bunches expect organizations to be mindful guardians of their own and other individuals' data.

2.3 The business Impact and Threats

As the world turns out to be progressively empowered through innovation and persistent association, organizations both vast and little should play it safe against being undermined through online stages (Harris et al., 2014). This is a critical business risk. Recent research from the Australian Small Business and Family Enterprise Ombudsman show a gloomy picture precisely that private ventures spoke of 43 percent of all digital assaults in the year 2018 (Cadieux, 2018). In the spate of ransomware assaults that happened in 2017, 22 percent of influenced organizations couldn't keep working (Cadieux, 2018). The attack was an eye-opener to organizations. It focuses to some central matters of section for criminals using online. Email phishing: attacks are hoax emails, designed and worded to appear from a trustworthy source, such as a bank or other financial institution (Wong, 2004: Cadieux, 2007: Harris et al., 2014). Wong (2004) notes that they aim to entice the recipient to click on a

malicious link that can lead to a viral infection of their systems, or ask the recipient to input data such as your login credentials for your bank which is then taken and used illegally.

- **Malware**: According to Cadieux (2007), this is a piece of the software sent to its target that, if opened or run, infects the machine or network. This can then be used to skim info from keyboards as keys are pressed, or provide external access to an unauthorized user in a remote location.

- **Ransomware:** According to Cadieux (2007) is delivered as above, but then locks your system or network down until a ransom (Money) is paid to restore access (Cadieux, 2007).

- A **denial of service:** According to Cadieux (2007) attack bombards the network with requests and locks up their system from its normal functioning. This is most of the time used by groups such as the hacker group Anonymous to shut down targeted sites .

Fewer than one in three businesses with less than 100 employees take active measures against cybersecurity breaches, and 87 percent of small businesses believe antivirus software alone is enough to protect them from the above (Cadieux, 2007). This is often not the case.
The first thing to examine is the potential entry points for attacks into systems and this can include point of sale systems, mobile devices used by staff, or allowing people to dial into your systems using a virtual private network (VPN). Once you are aware of where your business may be exposed, you can take appropriate action.

2.4 Impacts beyond Data Loss

There is an inappropriate hypothesis that cyber-attacks will cause probable damage to systems, and only technology will be affected, but the impacts can be far greater (Lewis, 2002). There are company measures such as insurance policies that cover some facets of a cyber-attack, but once an attack occurs and the damage is evaluated, there will almost certainly be areas that are not covered by such company policies. A potential attack could compromise data, premises, clients' data, ability to operate, or repute within the business network. Depending on the collateral damage, some of it will be covered, while some will almost certainly not be. It is important that companies do not take chances on issues of cyber threat.

2.5 Manufacturing Environment and Cybersecurity

A cybersecurity program and its supporting organization are not the reason that a business or government agency exists. In the case of a business, the company usually provides a service or a product. The business has certain information or systems networks that are vital to performing its service and producing its product. The purpose of a cybersecurity program, therefore, is to provide service and support to the business (Lee & Chao, 2016). To meet the needs of its customers, both internal and external to the company, it is imperative for the cybersecurity officer to understand the company and the company's business. This includes the following:

- History
- Products
- Business environment
- Competition
- Long-range plans
- Short-range plans
- Cost of business
- Product value

These are some of the most important parts of a business. In general, the cybersecurity program is not a product to be sold in the global marketplace unless that is the business of the corporation; it does not bring in revenue (Lee & Chao, 2016). In fact, cybersecurity is a cost to the business unless one can prove that the cybersecurity program is a value-added service that financially supports the business, assisting in bringing in revenue.

2.6 Creating Competitive Advantage through Cybersecurity

To ensure that the cybersecurity program supports the company's business services and products, the cybersecurity manager or officer must ponder on methods, values, and processes that will help the company in achieving a competitive advantage. Such methods and viewpoints should include a team approach (Lee & Chao, 2016). That is, have the company employees and especially management support the cybersecurity program. To help in that endeavor, the company should endeavor to insert, in suitable company policy documents, procedures that can help support their efforts. Business Managers and Cybersecurity

The role of the cybersecurity officer in managing a cybersecurity program is somewhat different from the role of the cybersecurity officer as a manager of the company. All company managers have some role to play that applies regardless of the manager's area of

responsibility (Conger, 1999). This also applies to cybersecurity officers in management positions. Establish and maintain a self-audit process to identify problem areas and take corrective action to eliminate deficiencies. These actions will drive the entire organization towards achieving the general organizational goals of the company. Companies that implement cybersecurity methodologies with every aspect of the company in mind are more likely to win the war against threats posed by cybersecurity. Remember that the cybersecurity program is a company program. That means help from everyone in the company is needed to ensure its success.

2.7 The Insider Threat

According to Schmid (2014), Organizations have long relied on security controls to diminish their disclosure to harmful acts by individuals within, and outside, its perimeter to an acceptable level. He stated that organizations have implanted more information technology into protecting their revenue, intellectual property and reputation. The big issue here is, if the organization fails to prevent, detect, and mitigate insider threats then the organizational has not dealt fully with cybersecurity problems (Schmid, 2014). Damages from insider activity, regardless of the intent, which most of the time are to cause harm to the organization can be very significant, and perhaps even crippling. Insiders may interrupt internal network activities, corrupt databases, and file servers, or deny the use of information systems and their data to authorized users. Stunning amounts of information can be stolen, lost, deleted, or corrupted literally at the press of a button (Shaw et al., 1998). For example, an individual who falsely have the thought that she may be fired deletes files from a computer system valued at $2.5 million (Kamm, 2008).The definition of an insider threat, thus emphasis on those individuals who have malicious intent(Shaw et al., 1998). This can cause a lot of fortune and revenue loss to an organization. Insiders may even collaborate with outside parties to receive technical support or to help identify useful information. The outcome from such activities may, in turn, result in substantial losses in corporate revenue and reputation (Österle & Otto 2014). Unfortunately, when talking about security risks, many pay ,much attention on the problem of perimeter security where they have seen marvelous advances in security technology, with innumerable dollars invested in perimeter security, encryption, antivirus systems, and content filtering, all of which aim to keep outsiders from damaging the organization. Paradoxically, most security specialists would agree the insider poses the greatest risk to information systems and is the most challenging threat to detect (Schemm, 2012).

Throughout this chapter, various issues pertaining to cybersecurity has been deliberated upon. It is quite clear from the various cited literature that, organizations over the years have invested huge sums of money in protecting corporate data and systems against threats posed from their external environment the results have not been much encouraging as a major canker: the insider threats still possess cyber challenges to organizations. Even though not much has been done on fighting the insider threats, organizations who are able to win the war using an appropriate methodology in implementing its cybersecurity programs have higher chances of winning the battle against cybersecurity. The next chapter focuses on cybersecurity measures and its implementation in manufacturing companies.

3. Cybersecurity in manufacturing Company.

Manufacturers are the creators, users, services, and installers of the things. Millions of interconnected devices are persistent throughout manufactured products and on the shop floors where they are made. Modern Technology is creating a massive prospect and driving transformative change in every economy. Manufactures are gradually becoming the backbone for most developed economies in the 21st century (Lapira, 2013). Technology has turned all manufacturers into technology companies (Lapira, 2013). The days of interacting with the customer only during a single transaction are over. Connected technology enables manufacturers to provide real-time performance monitoring and usage patterns for their customers throughout the entire lifespan of a product (Cobum, 2018). This will create a positive feedback loop resulting in better and more efficient products that will be sold and bought for their promise of measurable results. The current landscape of manufacturing companies has it that, companies are faced with new projects and new technologies each day. There is a need to implement these projects in a fast and responsive manner to win the market. This chapter thus focuses on the various methodologies for implementing projects in an organization. These methods are not conclusive in their analysis.

3.1 Project Management Frameworks

As already mentioned in the introduction above, companies are faced each day with projects that could cost from hundreds to millions of dollars. Project managers are thus tasked with carrying out projects within the specified cost, specification, and under schedule. This is often the maiden line for many project leaders and managers today. Without an operational project framework in place, it will not matter what one does in projects, it will undoubtedly be more complicated and troublesome (Westland, 2007). In this chapter, some project methodologies and structures used today across the industry, as well as the components that make up these project methodologies will be discussed. It is not always the case that project manager sticks to and adopt one project methodology, knowing various and diverse methodologies will help the project manager to identify the right and the best methodology for implementing projects successfully (Westland, 2007).

According to Lapira (2013), the very success of a company could depend on the successful outcome of its projects, so it becomes essential that the project manager minimize as much risk as possible and approach projects in such a way that it almost guarantees success. But how does the project manager do this?

One procedure is the tried and tested project methodology, which covers all possible areas when a project starts. Also benching the industry best and trending methodology is an appropriate way of getting the best. By retaining the right methodology, project leaders and managers are likely to deliver suitable solutions to their clients.

3.1.1 Selecting Project Methodology

Most companies in today's global business world have some form of framework for implementing their projects (Wiley, 2003). The intention of this section of the thesis is not to judge or assign credits to some particular methodology but instead elaborate some of the methods that some companies have adopted over the years and their benefits. Also, the chosen methodology: The PMI methodology is of much priority. Every company without a project management framework needs to build or select one before managing projects. According to Wiley (2003), If management wants their company to be successful in a project-based world, they should start moving and below are some factors according to Wiley (2003) that managers and organizations consider before selecting and sticking to a particular project management methodology.

- The overall company strategy of the company in line with market competition?
- The size of the project team assigned for the project or scope to be managed.
- The priority of the project.
- How critical the project is to the company.
- How flexible the methodology and its components are.

3.1.2 Best Project Methodology Practices

To guarantee a project's accomplishment through the entire adopted methodology, project leaders and project managers should keep to the following best practices as recommended by (Wiley, 2003) when building, tailoring or selecting a project management methodology:

- Use standard-proven processes and techniques.
- Acknowledge the best path for project implementation.
- Use best practices to reduce common pitfalls.
- Look at implementation time and cost reduction.
- Minimize excess templates and administration.
- Recognize what should and should not be implemented
- Draw on best industry practices and trends.
- Consult industry leaders and subject matter experts (SMEs).

3.2 System Development Life Cycle (SDLC) Methodology

System development lifecycle (SDLC) is a process of information system (IS) development. Various SDLC models have been created and can be implemented, including waterfall, rapid prototyping, incremental, Agile, spiral, fountain, build and fix, synchronize and stabilize and rapid application development (RAD) (Henderson, 1990). Many projects often follow the classic waterfall methodology, and it is fairly straightforward and easy to conceptualize.

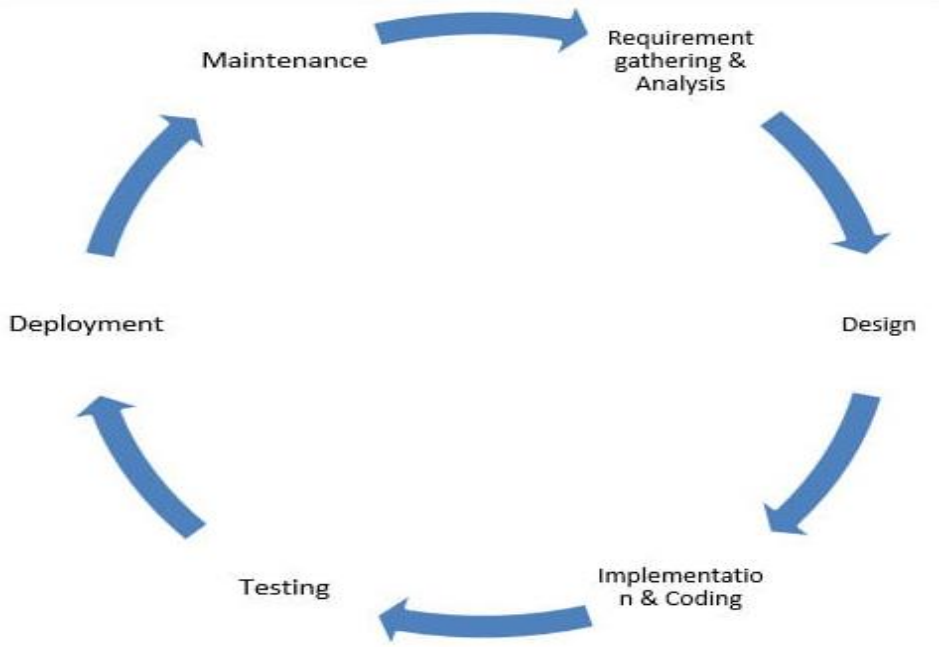


Figure 1: Phases of SDLC

Source: Henderson, 1990

- **Requirement Gathering and Analysis**

  Amid this stage, all the significant data is gathered from the client to build up an item according to their desire. Any ambiguities must be settled in this stage as it were. Business analyst and Project Manager set up a gathering with the client to assemble all the data like what the client needs to build or develop, who will be the end user, what is the reason for the product. Before building a product, understanding of the product and it's significance is very essential.

- **Design**

  In this phase, all the necessarily requirement put together in the SRS document is used as an input and software architecture that is used for implementing system development is derived.

- **Implementation**
  Implementation begins once the developer gets the Design document from the client and gather all information. The Software design is translated into the source code by the developer. All the components of the software are implemented in this stage.
- **Testing**
  Testing begins once the coding is finished and the modules are discharged for testing. In this stage, the developed software is tried altogether and any imperfections found are allocated to designers to get them fixed. Retesting, regression testing is done until the test meets the clients specification.
- **Deployment**
  At the point when the item has at last pass the testing stage, it is sent in the generation condition or first UAT (User Acceptance testing) is finished relying upon the client's desire. By virtue of UAT, an imitated creation condition is produced, and the customer close by the engineer does the testing. In the event that the client finds that the item meets every one of his determinations and prerequisites, at that point he signs that the item Go live.
- **Maintenance**
  After the deployment of the product on the production environment, maintenance of the product for example in the event that any issue comes up and should be fixed or any improvement is to be done, the developer make the necessary changes.

For many SDLC-type projects currently, the trend and style of these techniques most often involve finishing one stage after the next. Many are monolithic in nature; they are time-consuming (Alexander, 2005). In today's complex technological world, where faster is better and part of the general project goals, project managers struggle to complete projects where complex, unknown technologies are being used. Clients do want to see results much earlier than before (Alexander, 2005). Most methodologies that follow the SDLC discuss below.

3.2.1 Waterfall model

As the very first model to be discussed under the SDLC. The waterfall model can also be referred to as the linear sequential model. In this model, the output of one phase is the input for the next phase. That is to say, following the general SDLC pattern, a gathering of the requirements is done at the initial stages. It is only until

this face is fully completed then the design stage is started.

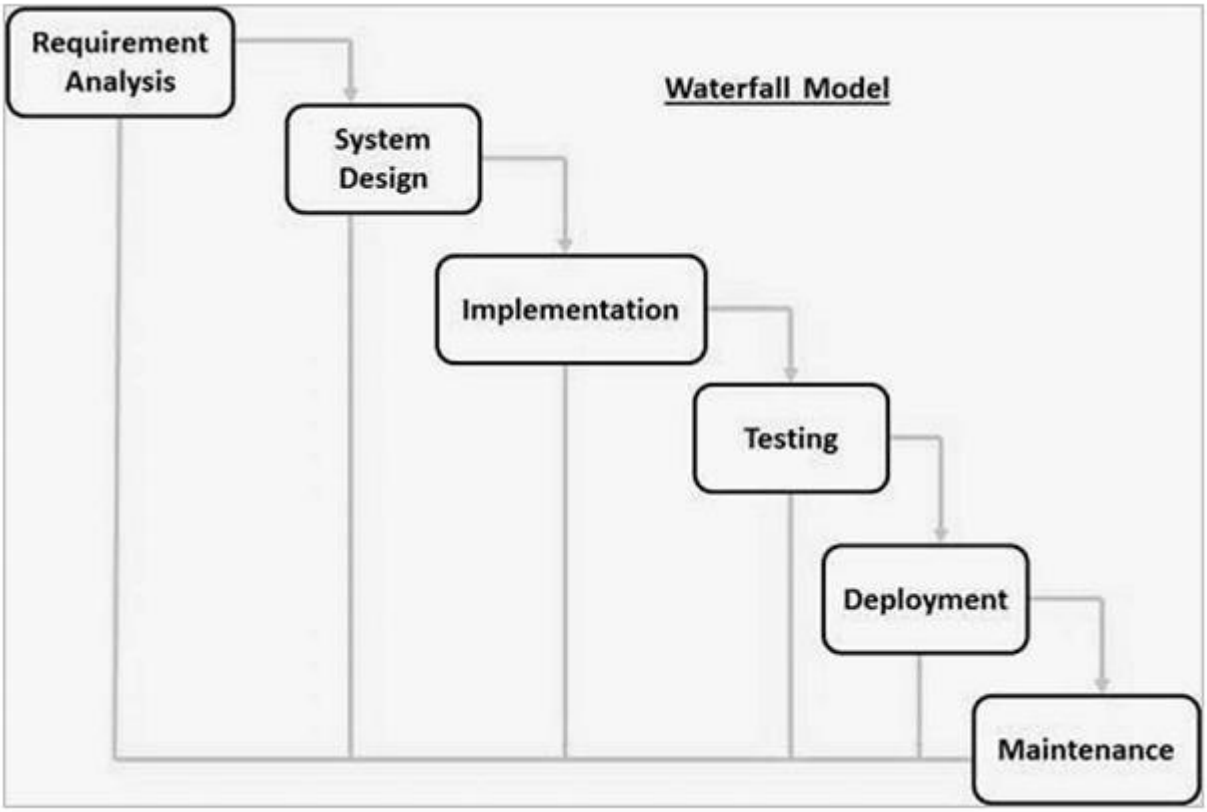


Figure 2: The Waterfall Model

Source: Balaji & Sundararjan, 2012

When the design stage is successfully completed then the implementation phase is started. This pattern is followed until the final project is moved to production and continuous maintenance is done for continues improvement of the project. One limitation of the waterfall model is that the waterfall model that it demands a lot of time to complete a project and hence its not suitable for smaller projects that has limited time in its delivery(Alexander, 2005).

3.2.2 Spiral Model

Another model under the SDLC is the spiral Model. This model includes iterative and prototype method. Spiral model phases are followed in the iterations. The term loops in this model denote the phase of the SDLC process i.e. the innermost phase is of requirement gathering & analysis which follows the Planning, Risk analysis, development, and evaluation.

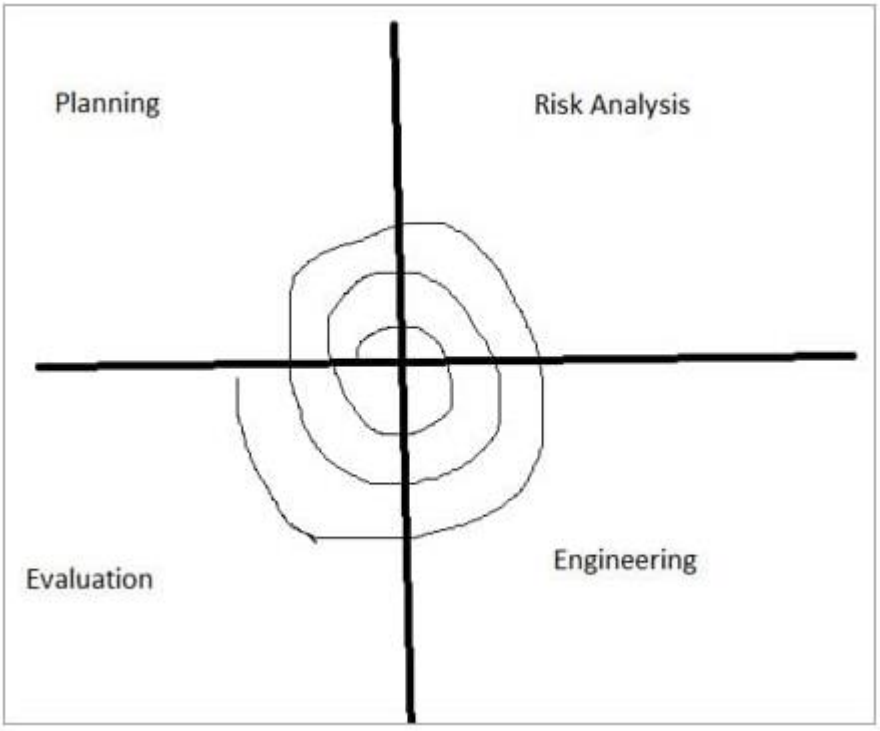


Figure 3: Phases of the spiral model

Sources: Boehm, 1988

Next loop is designing followed by Implementation & finally testing. The planning stage includes requirement gathering wherein all the required information is gathered from the customer and is documented. Project requirement specification document is created for the next phase. In this phase, the best solution is selected for the risks involved and analysis is done by building the prototype. Once the risk analysis is done, coding and testing are done. Customer evaluates the developed project and plans for the next iteration. In the spiral method, the cost can be high as it might take a number of iterations which can lead to high time to get to the ultimate product.

3.2.3 Iterative Incremental Model

Another important and common model is the iterative incremental model divides the product into small chunks. Feature to be established in the iteration is decided and executed. Each iteration goes through the phases namely Requirement Examination, Designing, Coding, and Testing.

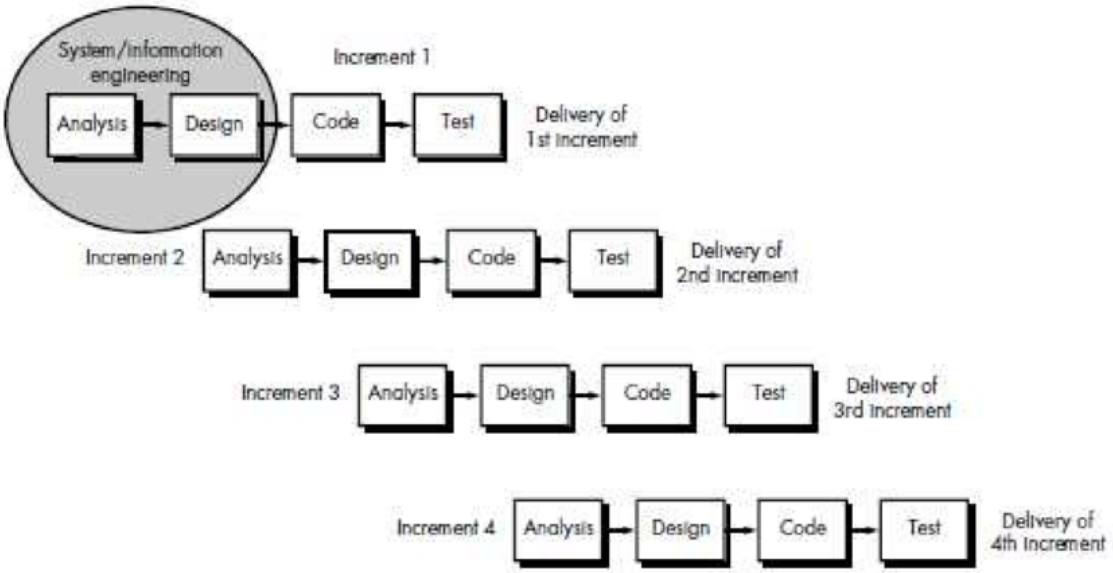


Figure 4: The iterative incremental model

Source: Olajide, 2016

Definite arranging isn't required in emphasis. When the emphasis is finished, an item is checked and is conveyed to the client for their assessment and input. Client's criticism is actualized in the following emphasis alongside the recently included component. Subsequently, the item augments as far as highlights and once the cycles are finished the last form holds every one of the highlights of the item.

3.2.4 The Agile Model

According to Potter and Kramer (2019) Agile Model is a combination of the Iterative and incremental model . This model concentrates more on flexibility while developing a product item instead of on the prerequisite. In Agile, a product is broken into small incremental forms. It isn't created as a total item in one go. Each increment in terms of features. The following form is based on past usefulness. In agile each sprint lasts for 2-4 weeks. At the end of each designed sprint, the product owner confirms the product and approves and it is delivered to the client. Client feedback is taken for development and his proposals and improvement are worked on the next sprint. As of now, numerous organizations support agile methodologies presenting new nontraditional way of structure complex items and frameworks.(Henderson, 1990). Manufacturing companies that use agile methodologies include financial, IT, telecom, utilities, and a lot more administration ventures. Besides, this pattern is beginning to develop around the world. Coming up next are the most commonly used agile methodologies:

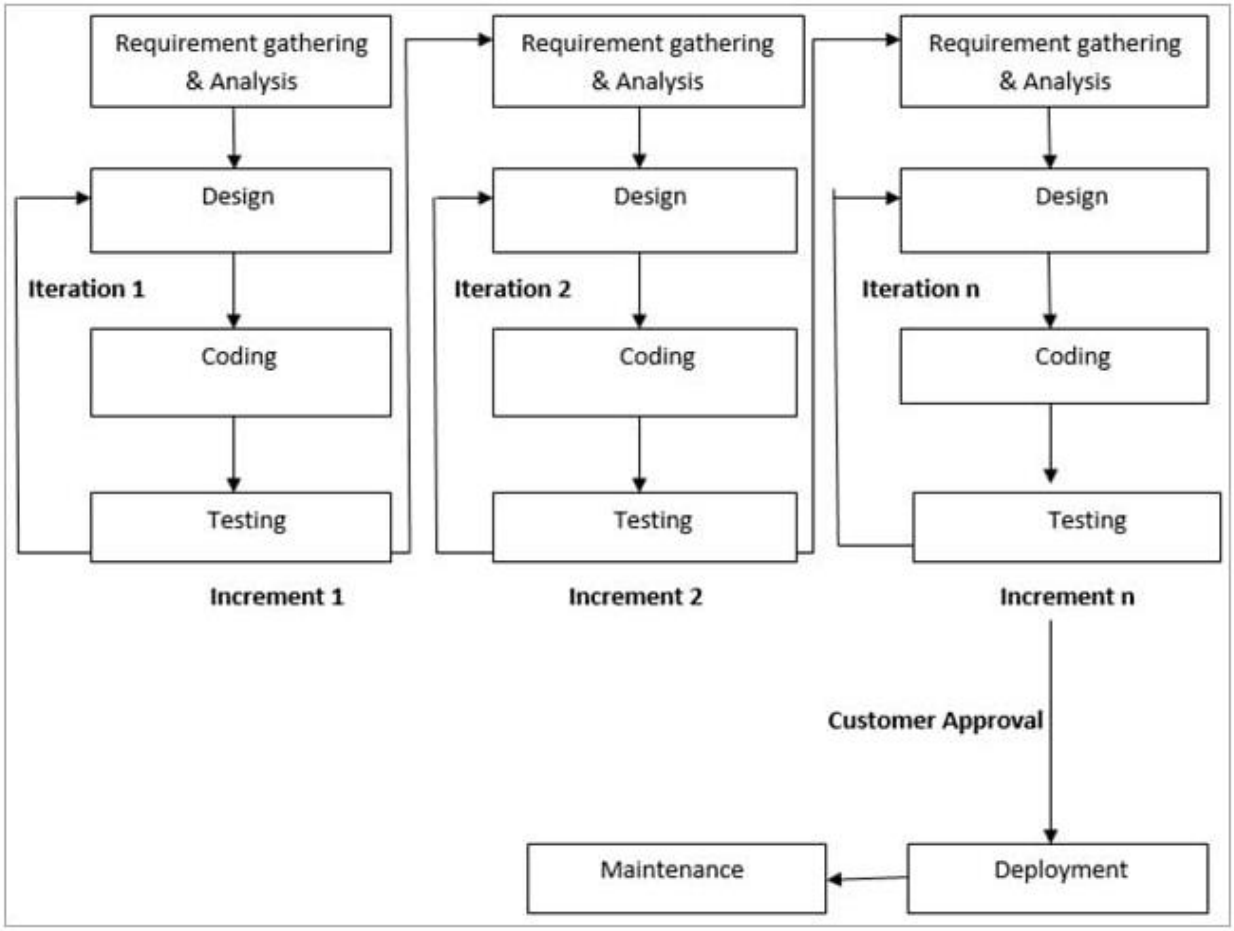


Figure 5: The Agile Model

Sources: Ambler, 2004

One very important of this method is that Customer satisfaction as the feedback and suggestions are taken at every stage. Notwithstanding, If a client is not clear about what exactly he/she wants the final product to be, then the project is more likely to fail.

Every process has its limitations or problems and the System Development Life Cycle (SDLC) is no exception. Most SDLC models or methods which were not mentioned for the purposes of time and space are designed around a business partner or customer requirements. It is difficult, however, for business partners and customers to relay the level of detail required for systems to be developed as per their expectations

- Extreme Programming (XP).
- Scrum.
- Crystal methodology.
- Dynamic Systems Development Methodology (DSDM).
- Rapid Application Development (RAD).
- Adaptive software development.

- Lean development.
- Feature-driven development

Agile methodologies better suit small projects where smaller project teams are involved. Many smaller companies do not use heavyweight methodologies and prefer the more agile approach to building solutions

3.2.5 Extreme Programming Methodology

XP, one of the new encouraging types of lightweight techniques, is the brainchild of Kent Beck. XP is one of the spry procedures (Henderson, 1990). It has gotten such a great amount of consideration as of late that a portion of the worldwide task associations is checking on it for incorporation in their technique portfolios. It depends on emphasis that typify a few practices, for example, little discharges, straightforward plan, testing, and consistent joining. XP groups utilize a basic type of arranging and following to choose what ought to be done straighta way and to anticipate when the venture will be done. XP grasps four guiding principles that its task groups ought to pursue:

- Communication
- Feedback
- simplicity, and
- Courage.

The attention is on business esteem, where the group delivers the product in a progression of little, completely incorporated discharges that breeze through every one of the tests the customer has characterized.

3.2.6 The Scrum Methodology

The purpose of scrum is to restart play quickly, securely, and genuinely after a minor encroachment or stoppage (Schwaber, 1997). A SCRUM is a team pack, where everybody in the team works together. It delivers the project within time and with minimum expense (Mahalakshmi, 2013). From a strategy perceptive, Scrum alludes to the system utilized in rugby for taking care of business out-of-take care of business once more into play. Scrum is a lightweight, coordinated system concentrating on programming improvement. Scrums two pillars are tea, empowerment and adaptability. The Scrum framework is heuristic; it depends on continuous learning and change in accordance with fluctuating factors. It recognizes that the group doesn't know everything toward the beginning of a venture and will develop through understanding. Scrum is organized to help groups normally adjust to changing

conditions and client prerequisites, with re-prioritization incorporated with the procedure and short discharge cycles so your group can continually learn and improve (Schwaber, 1997).

3.2.7 Dynamic Systems Development Methodology (DSDM)

he DSDM, created in the United Kingdom, depends on Rapid Application Development (RAD) that utilizes prototyping emphasis to convey ventures Wong 2009: Charvat 2003). This model has a few viewpoints that vary from the most widely recognized models. The thing that matters is that time and assets are fixed and the usefulness of the deliverable is variable. In different models, the usefulness (or item) is fixed, and assets and time are, partially, adaptable. Organizations today center around finding the correct arrangements rapidly. DSDM gives an undertaking system to make this goal attainable. DSDM's objective is speed yet not to the detriment of value. DSDM is autonomous, guaranteeing that it is versatile to address the issues of any association. The effortlessness, common sense, and adaptability of the methodology are reasonable for sellers, SMEs, advisors, etc, making DSDM applicable over an assortment of enterprises. Amid the useful model cycle, first-pass portrayals of the new or changed procedures are created for refinement.

According to Charvat (2003), a pilot project is created during the design and build iteration. All through the development, feedback is used to assess and refine the procedures so they can be taken off to the more extensive advancement population with confidence that they will accomplish the advantages expected of them. Execution of procedures includes huge correspondence and preparing of the venture staff. Since correspondence is significant all through the advancement of improved procedures and their last conveyance, a correspondence methodology is added to the standard DSDM item set. The structure of procedure improvement teams is described based on DSDM product set. As always, the visionary role is an important one in keeping the focus of the work aligned to the needs of the organization (Charvat 2003).

3.2.8 Rapid Applications Development (RAD) Methodology

Sometimes users want to see a product they understand and not wait for development to go off the building line (Charvat 2003). Outmoded software development techniques usually follow a sequence of steps with signoffs normally at the end of each stage. This grouping may be:

- User requirement gathering
- Specifications and the design formulated.
- Development starts and the project Is completed. is finished.

• Testing commences.

This process can be time-consuming ,but shorten the approach. In any case, what occurs in the event that you find amid the advancement stage that the innovation doesn't work? This has monstrous repercussions for the whole straight methodology, and such a technique could make the task fall flat. The time passed between the plan and improvement could keep running into numerous months or worker hours. Customers are then frequently reluctant to assume such a misfortune except if it is a piece of their key business technique. Undertaking directors need to utilize an undeniably progressively powerful methodology or venture approach for advancements that are untested or fall into a high-chance classification. The RAD methodology may be the most reasonable to realize immediate benefits (Charvat 2003).

In this chapter some familiar methodologies and models for implementing projects by various organizations have been discussed. The techniques are not exhaustive and conclusive in their explanationss, however, the PMI methodology which is our chosen method for the purposes of this thesis will be discussed in the next chapter and using a real-time company followed how implementation of cybersecurity program is done.

4. Project Management Using PMI Methodology

The previous chapters helped the reader to understand the threats that are been posted to manufacturing organizations as a result of the speedy and ever-changing business world. Also, the concept and importance of organization data have been discussed. Insider threat- a key concept that comes to play and that has cost the most organization to lose huge sums of money has been disused. In this chapter, much focus will be lay on how Foxconn, a manufacturing company can implement cybersecurity measure using the PMI approach.

PMI states that the application areas and the environment in which the project will be run in necessary for successful completion of the project.

While the previous chapter followed the recommendation from PMI, this chapter will get in detailed specifics of managing the cybersecurity implementation project. Hence it will be important to understand the PMI methodology. The chapter will start by introducing the PMI methodology to the understanding and then getting the specific cybersecurity to different department project. Terms, processes, and steps in the PMBOK, will be explained and linked to the cybersecurity implementation project, to enable the reader to see the link and be able to apply PMI standards and recommendations in managing the project.

4.1 Defining PMI Methodology

Project Management Institution (PMI) is one of the world's largest professional membership associations, with over 500000 members and credentials holders in more than 300 countries IT is not for profit organization that advances the project Management profession through globally recognized standards and certifications, collaborative communities, an extensive research program, and professional development opportunities (Project Management Institute, 2017).

According to the PMBOK (2017), PMI has a global standard which provides guidelines, rules, and characteristics for project, program and portfolio management. These standards help the organization to achieve professional excellence if consistently applied. PMI Standards are widely accepted in many countries. This helps the project managers on which actions to take in various stages of the project

4.2 Project Management Body of Knowledge

The PMBOK (2017) describes the knowledge unique to the project management discipline, overlaps other management disciplines. According to the material in the PMBOK (2017) Guide is a subset of the larger Project Management Body of Knowledge. The following project management knowledge is described within the Guide:

4.2.1 Five Project Management Process Groups:

- Initiating
- Planning
- Executing
- Monitoring and controlling
- Closing

4.2.2 Knowledge Areas of Project Management

- Integration Management
- Scope Management
- Time Management
- Cost Management
- Quality Management
- Human Resource Management
- Communication Management
- Risk Management
- Procurement Management
- Stakeholder Management

4.3 The reason for choosing PMI methodology

- PMI has widely accepted methodology worldwide.
- By using a standard methodology it ensured consistency in cooperation with the project managers managing subprojects within the project.
- Most project managers, managing the subprojects within the cybersecurity project has a PMP certificate or PMP associate certificate.
- The PMI standards will ensure successful completion of the project if efficiently applied

4.4 General management Knowledge and skills

According to the PMBOK(2017), the general management knowledge and skills Provides the foundation of building project management skills and is often essential for the project manager. General knowledge and skills encompass planning, organizing, staffing, executing and controlling the operations of an ongoing enterprise. This knowledge increases the probability of the project Manager managing the project successfully.

4.4.1 Application Area Knowledge, Standards and regulations

According to the PMBOK (2017), application area refers to the knowledge, standards, and regulations specific to an application area that are not needed or present in other projects. Application areas are categories of the project that have significant common elements not found or used in all projects. These areas are usually defined in terms of the following:

- Functional Departments and supporting disciplines
- Technical elements such as software development,
- Management Specialization such as government contracting
- Industry group such as automotive, chemicals, agriculture, or financial services.

4.4.2 Cybersecurity Implementation application area: IT security

Cybersecurity implementation project falls under the area of IT security, to be specific making sure information systems are kept from theft or damage to hardware and software. Knowledge area in this will be required by the project manager and subproject managers working in this area. They need to understand clearly the difference between primary and secondary controls. It is also crucial to understand but not limited to the following terms in this application area:

- Cyber-Physical Systems
- Cross-Cutting Security
- CPS Domains

Foxconn as a manufacturing company has many security standard documentation which could enhance this understanding. A good IT security book can be useful.

4.4.3 Cybersecurity application area: organization change

Change management is an approach to shifting/transitioning individuals, teams and organization from a current state to a desired future state. It is a process in an organization that ensures that stakeholders accept the change and the new state.

Managing this project requires the basic understanding of organization change if this change is applied globally in an organization for Foxconn is it both at strategic an operation level

4.4.4 Understanding the project environment

According to Schemn (2010), all projects are planned and executed within the social, economic, and environmental context. It is important for the project team to be cognizant of this context and consider project impacts.

- **Cultural and social environment**

  The project is huge and global so it's important to understand the cultural differences. It is also crucial to understand the organizational culture of the IT service delivery the project is being carried out.

- **The international and political environment**

  Due to the global nature of the project and the fact that the project involves many countries, it is important to plan international way and no single project manager can manage the whole project alone, so it is good to divide it into subproject and appoint subproject managers.

4.5 Interpersonal skills

The management of interpersonal skills that are necessary to ensure that the cybersecurity implementation project is successfully completed includes:

- **Effective communication:** exchange of information, the project has a lot of stakeholders and communication is key to success

- **Influencing the organization:** The ability to get things done**',** this is the key since they will be a lot of people affected and may need to ensure things get done.

- **Leadership:** rising a vision and scheme, and inspiring people to accomplish the vision and strategy.

- **Motivation:** Stimulating people to achieve excellent performance and to overcome obstacles to change

- **Negotiation and conflict management -**conferring with others to come to terms with them or to reach an agreement. Conflicts always arise in such a global project and it is necessary for a project manager to be able to resolve the conflicts**.**

- **Problem-solving -**the mixture of problem definition, alternatives identification and analysis, and decision making**.**

4.6 Project Life Cycle and Organization

Project managers and leaders sometimes can break the whole project into units or phases with connections to the ongoing operations of the performing organization. Many organizations identify a specific set of life cycles for use on all of their projects and for Foxconn the projects cycles follow the following four stages.

- **Initiating** (starting the project): Phase when the project is started, starting from the project charter, kick-off meetings with key stakeholders (starting the project)

- Planning (Organizing and preparing): Phase for planning, planning how the project is going to be run.

- **Execution/Implementation** (Carrying out the work including monitoring and controlling): Phase where the project work is actually carried out, the propjet manager and the project management team monitors and controls the work.

- **Close-out/Termination/Final**: this is the stage where the project is concluded, intellectual capital and lessons learned collected.

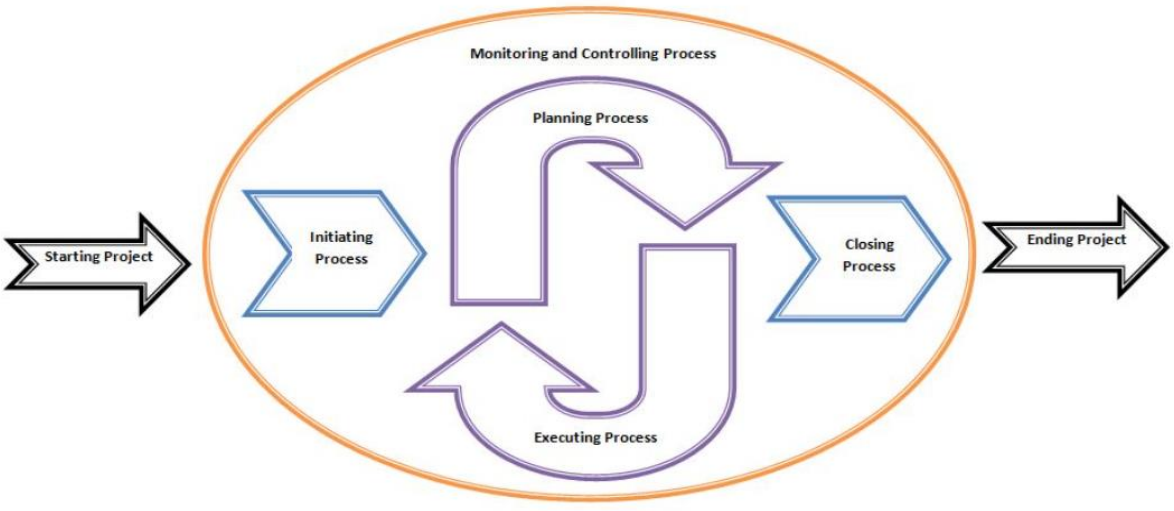


Figure 6: Monitoring and Controlling Process

Source: Muehlen, 2000

4.6.1Characteristics of Project Life cycle

According to the PMBOK (2017), the following phases of are defined from the begining to the end of a project.

- Describes the stages of a project from start to the end.
- Usually, some form of technical hands off occurs when transitioning between one phase of a project life cycle to another.
- In general, deliverables from one phase are reviewed for correctness and wholeness before the next phase begins. However, phases can overlap. The practice of overlying phases is an example of program compression called fast tracking.
- Differs based on industry, application area. Usually speaking, project life cycle defines:
    - The technical work to be done in each phase
    - When the deliverables are to be generated in each phase and how each deliverable is to be reviewed, verified and validated.
    - The skills involved in each phase(the who)
    - How each phase is controlled and approved.
- Most project; life cycle description share a number of common characteristics:
    - According to the PMBOK (2017), phases are sequentially and usually involving the transfer of technical information to hand off a technical component.
    - According to the PMBOK (2017), cost and staffing levels are low at the start, peak during the intermediate phase, and drops rapidly as the project nears conclusion(PMBOK,6^{th} edition, 2017),
    - According to the PMBOK (2017), the probability of successfully completing the project I slowest at the start of the project. Hence, risk and uncertainty are highest at the start of the project Generally speaking; the probability of a successful completion progressively increases as the project continues.

- According to the PMBOK (2017), the ability of all stakeholders to influence the final characteristics of the project product is highest at the start of a project and becomes progressively lower as the project continues. This can largely be contributed to the increased cost of change and error correction as the project develops(PMBOK,6th edition).

- Each project phase is marked by the completion of one or more deliverables.
- Phases can be further divided into sub-phases. Each phase is concluded with a review of the key deliverables and project performance to determine if the project should proceed to the next phase and to detect and correct costly errors. These phase end reviews are often called phase exits, milestones, phase gates, decision gates, and stage gates/kill points.
- In order to consistently control a project in order and ensure success, the appropriate level of governance should be implemented. The governance activities are described in detail within the project management plan.
- The practice of overlapping project phase when the risks are deemed acceptable is called fast tracking.
- Subprojects within projects may also distinct project life cycles which follow the same lifecycle.
- The driving force within projects may also have distinct project life cycles.
- Differencing between project life cycle and product life. For example, a project to deliver a new computer system to the market may be one phase or stage in the product cycle. The product life cycle could consist of several follow-ups enhancements (via unique projects) for this computer system before the product reaches the end of life phase (stage).

4.6.2 Project Stakeholders

Project Stakeholders are individuals or organizations: -

- Who is actively involved in the project
- Whose interest may be positive or negatively affected by the outcome of the project execution or completion

- Who may exert influence over the project and its results

The project team must identify the stakeholders, determine their requirements, manage them as well as influence those requirements to ensure a successful project. Project Stakeholders have various levels of responsibility and authority and these may change over the course of the project ‘s life cycle. Identifying project stakeholders is not an easy task.

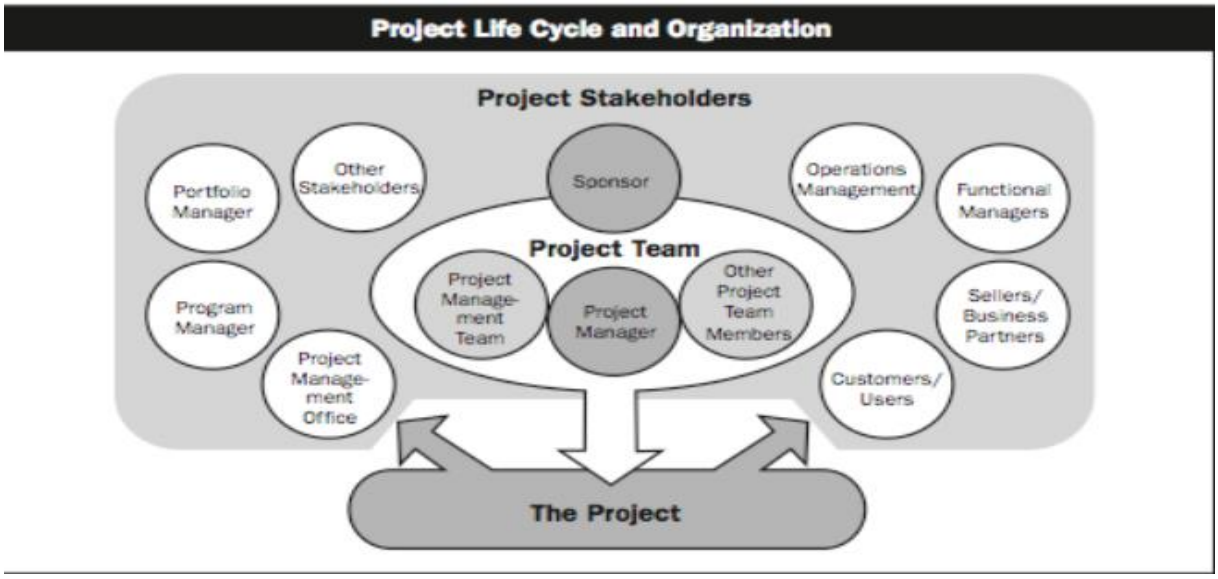


Figure 7: The relationship between stakeholders and the project

Source: (PMBOK, 6th edition, 2017)

4.4.1 Project Global implementations of Cybersecurity project stakeholders

- Overall Project manager (Ruvimbo Jefrey)
- Customers -customers who we handle their data
- Project Team (IT specialists, System administrators, Managers)
- Project management Team (Subproject project managers and team leaders)
- Sponsor: IT Security Global director
- Influencers (Delivery Project Executive, Service delivery managers)
- Project Management Office
- It Security Service leaders

- Global Managers

4.7 Organizational influences

Project is predisposed by the organization set up. The project can also be swayed by the maturity of the organization with respect to its:

- Existing Project management systems (as related to the organizational system, below)
    - Culture and style of the organization
    - Organizational existing structure
    - Project Management Office and layouts

4.7.1 Organization Structures

As explained Foxconn has a multidimensional matrix organization structures sometimes referred to as composite. The composite organizational structure ensures that Foxconn has the advantages of both functional, Matrix and Projectized organizational (PMBOK, 6th Edition, 2017).

- Like a matrix organization, it has the following benefits: Better project manager control over resources compared to the functional organization, rapid response to possibilities, enriched harmonization effort across functional lines, people have a home after the project is over, etc.
- Like projectized organization, it has the following advantages:
    - Most of the organizational resources are involved in project work.
    - The project leader has a boundless deal of independence and authority
    - Departments report directly to the project manager.

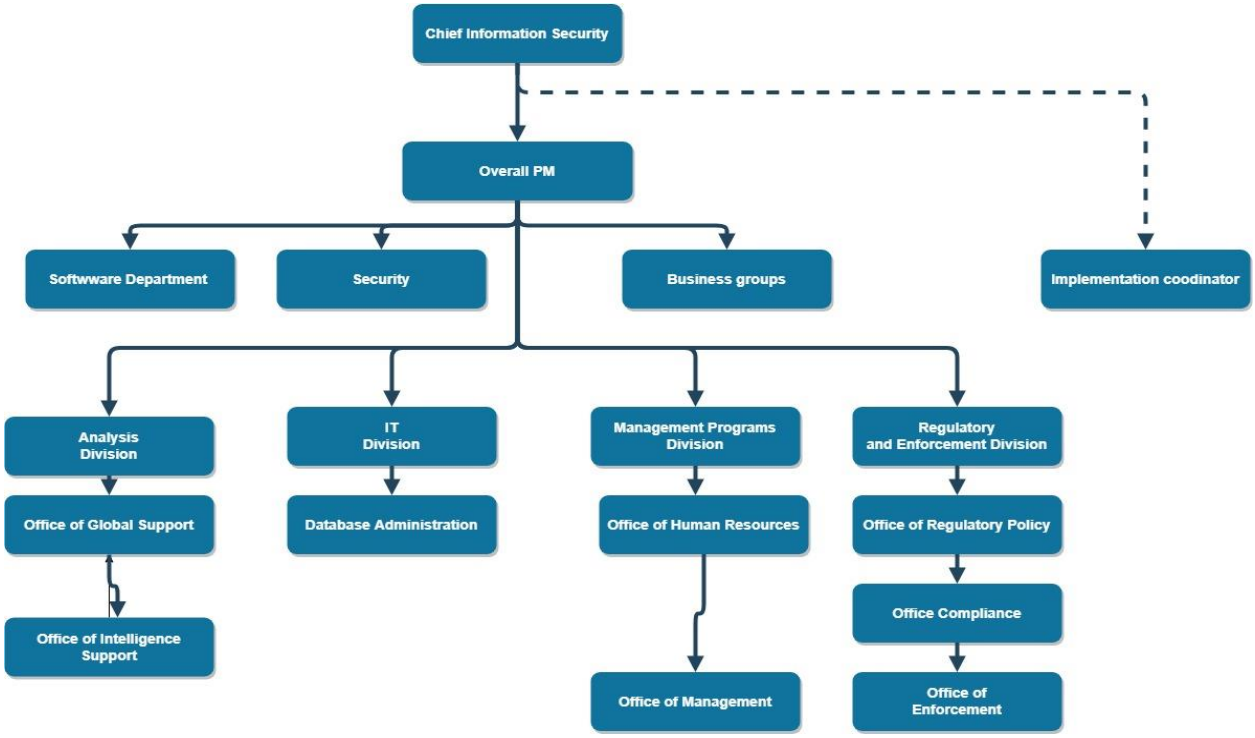
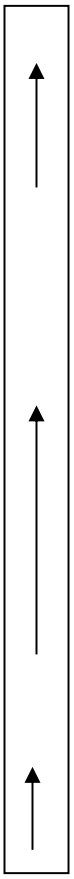


Figure 8: Global Cybersecurity Project OBS

Source: Own work

4.8 The initial Project Decision structure



1. The Project Sponsor/Owner is the decision taker related to
    - Change in Project Scope
    - Change in Milestone plan
    - Project external) risks and issues not solved by the Sponsor
    - Approve Deliverables
    - Handle Project external *) risks and issues
    - Approve Business case and Project budget
2. The Project Manager is the decision taker related to
    - Proposed changes
    - Project problems/issues
    - Identified risks
    - Project Schedule
    - Assign and un-assign project resources
    - Deliverables
3. The Core-Team-members are the decision takers related to
    - Production of documentation; developments and other project items within his/her assigned functional Area.

4.9 Project Processes

For a project to be effective and successful, the project manager and team must: -

- Select suitable processes within the process groups that are necessary to meet project objectives.
- Use a defined method to familiarize the product terms and plans to meet project and product necessities.
- Conform with requirements to meet interested people needs, wants and expectations
- Balance the rival demands of scope, time, cost, quality, resources, and risk to produce a quality product.
- Projects are composed of procedures. According to the PMBOK (2017), a process is a series of interrelated actions and activities that are performed to achieve a product, service, or result.

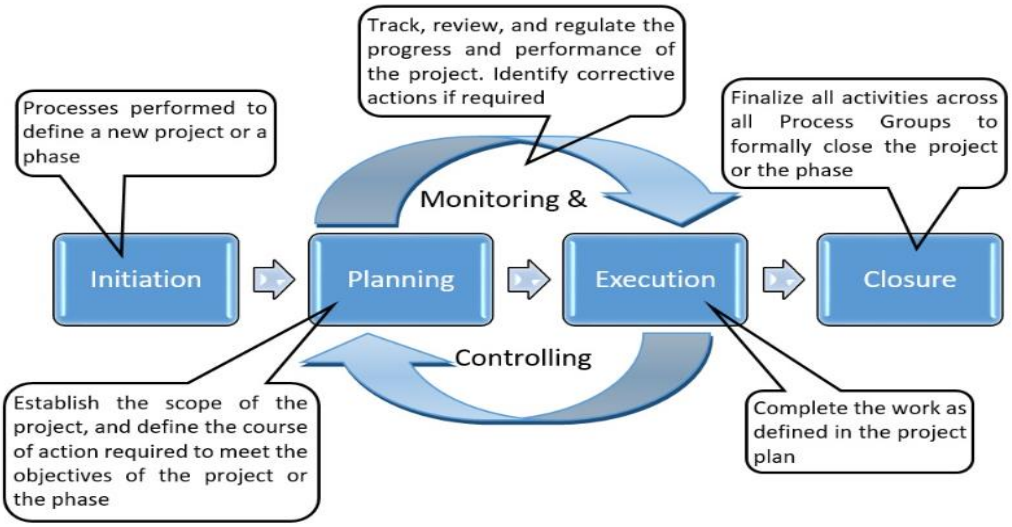


Figure 9: Overview of Project Management Process groups

Source: PMBOK, 4th Edition, 2008

4.9.1 Initiating Processes

Defines the project or phase and authorizes the project phase.

- **Develop Project Charter**

  A Project Charter is a document that authorizes the project and gives the project manager authority to assign resources. In the global cybersecurity project, the project charter was prepared by the consultants at a strategic level and handed to the project manager.

- **Identify stakeholders**

  Identifying and analyzing project stakeholders are key to project success. Key stakeholders on the project were identified as listed in section 4.8.4. Stakeholders needed to be managed to ensure those who are affected by the project and those who have the power to have a negative impact on the project, are properly managed.

Table 1: Stakeholder's analysis for Foxconn cybersecurity project

Stakeholder	Stake in the project	Interest	Current support for this project	Stakeholder Management Strategy
IT security Director	Project Sponsor	High	Key stakeholder and supporter of the project	Involvement in project weekly sponsor meeting
Overall project managers	Project managers	High	Work to ensure project success as his reputation is on the line if work not done	Already motivated to work
Subproject managers	Sub-project Managers	Medium	Work to ensure project success as his reputation is on the line if work not done	Already motivated to work
SWD Support	Own the software used	High	Want to make sure proper software is used	Weekly meeting
Security	Perform the work	High	Owns the work being done	Weekly meeting
HR Support	Have customer data	Medium	Make sure proper resources are hired	Bi-monthly meeting
Legal support	Knows legal areas of project	Medium	Make sure work is done according to the specific country laws	Bi-monthly meeting
Security Coordinator	Manage steady state	High	Want to make sure the work is done on time	Weekly meeting
ICT	Current perform the work	Medium		Bi-monthly meeting
DPE	Have contact with Customer	High	Want to ensure that the cost of work remains the same or becomes cheaper	Bi-monthly meeting
Customer	They pay for the work being done	High	Want to ensure the continuation of support without interruption	Update for the DPE

Source: Own work

4.9.2 Planning process group

"The planning process Group which I did for the cybersecurity project in Foxconn involve of those methods performed to launch the total scope of the effort, define and refine the objectives, and budget of project as well as additional plans to manage the overall project; and develop the course of action required to attain those objectives. The planning processes develop a project management plan and the project document as that will be used to carry out the project Reference. Having a successful pass through this group of processes helped me as a project manager in managing the project stakeholders and in getting support from the

stakeholders. The Planning process group covered all 10 knowledge areas over the duration of the project" (PMBOK, 4th Edition, 2008, p.46)

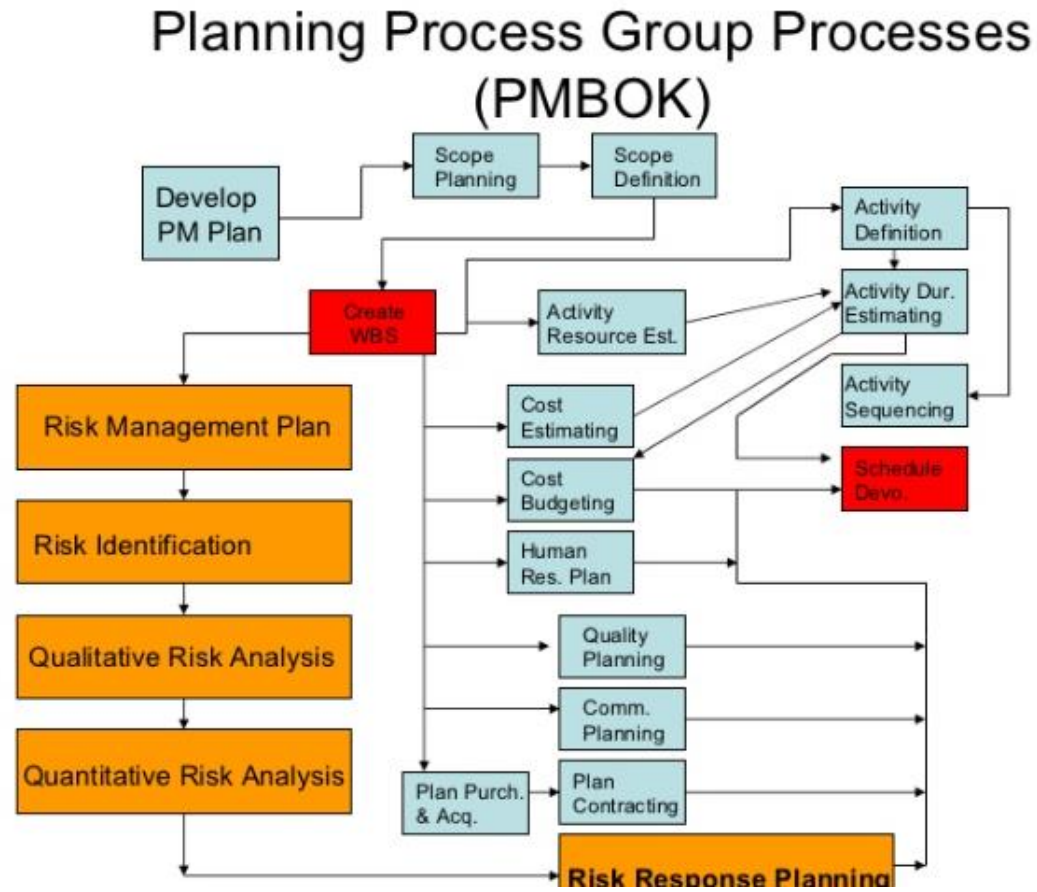


Figure 10: Planning Process Group Processes

Source: PMBOK, 2004

4.9.3 Develop a project management plan

Project management plan consists of a number of sub-plans, for example, risk management plan, change management plan and communication management plan. The actions are necessary to define the interactions with a subsidiary plan. The project management plan is the source of how the project will be run**.**

4.9.4 Collect requirements

This is the process to collect and document the needs of the stakeholder in order to meet the objectives of the project. In the cybersecurity project, the following techniques were used to gather the needs of the stakeholders: -

- Kickoff meeting with the identified stakeholders: -this allows me as a project manager to share details from the cybersecurity implementation project and the stakeholders were able to brainstorm and identify the missing stakeholders.

- Face 2 Face interview was also used to get the information.

- The project control book was used to document the findings

4.9.5 Define scope and activities

- The process of developing a detailed description of the project and the project flow is called: define the scope.

- The process of identifying the specifications to be performed in order to produce project deliverables is called define activities (PMBOK, 6th edition, 2018**).**

In this project, the scope and list of activities as shown in subsequent chapters were defined using various workshops between different teams in different locations; who worked closely with project managers to define scope and list for activities.

4.9.6 Estimate activity resources and duration

These are two processes according to PMI that where combined in this project. This involved the estimation of the type; quantities of materials and people needed to perform the project work and produce deliverables. Estimation is the process of approximating the duration of work periods, needed to perform a particular activity.

The two main outputs of these procedures are Activity resource requirements, resource Break structure, and activities duration evaluations.

- **Develop Schedule**

  This is the process of analyzing the activity duration resource requirements and schedule constraints to create the project schedule the main output for this process is the project schedule and the schedule baseline. Below is an example of a high-level plan for the project**.**

Table 2: High-level project plan

Milestone	Start Date	End Date
Project Planning		
PDR Creation	20/04/18	10/5/18
PDR Approval by Project owner	02/04/18	10/4/18
PDR Approval By Executive Sponsor	02/04/18	10/4/18
Human Resource Allocation	02/04/18	10/4/18
Wave 1 at Factory	**13/04/18**	**30/010/18**
Kick off meeting	**02/04/18**	**02/04/18**
Human Resources Allocation	**02/04/18**	**10/04/18**
Phase 1(Implementation of Technical solution)	**02/04/18**	**16/04/18**
Define Initial Project Scope Wave 1	02/04/18	10/4/18
Obtain exception approvals if needed	02/04/18	29/04/18
Policy Implementation	02/04/18	30/05/18
Identify Accounts to be used	02/04/18	29/4/18
Identify Process/ Procedures/ Documentation to be used	13/04/18	19/05/18
Identify and define work to be done	02/04/18	19/05/18
Identify privileges required for management of activities identified	02/04/18	19/05/18
Identify Cybersecurity operations	02/06/18	19/08/18
Assess/define the management structure to be applied to cybersecurity in the organization	02/08/18	19/10/18
Obtain Stakeholder and CSL approval for transfer	20/10/18	09/11/18
Transfer Costing Model	27/11/18	13/12/18
Educate security employees on new tasks	02/12/18	13/01/19
Validate successful training	14/01/19	23/1/19
Obtain stakeholder sign off for successful transfer	23/01/19	30/01/19

Phase 2(Other applications)	**02/01/19**	**30/04/19**
Wave 2(Implementation of cybersecurity)	**12/01/19**	**30/04/19**
Phase 1 (Operating Systems)	**12/04/19**	**30/04/19**
Phase2 (Other Applications)	**15/04/19**	**30/04/19**
Project Closing	**15/06/19**	**15/06/19**

Source: Own Work

- **Effort Estimates and determine a budget**

These are two processes according to PM, but in the most project, they are carried in parallel. Estimate cost is the process of making an approximation of the monetary value of activity needed to perform the activities. After that, the cost is aggregated to determine the cost baseline. The estimation was done using bottom-up estimation, which means that the sum of individual activities is summed up to come up with a total estimation. In the project are two kinds of estimations should be carried out: -

- Estimation of the project activities: This is the work to be carried out to ensure completion of the project activities.
- Estimation of the cybersecurity activities, in the centralized team

4.10 Project activities Estimations

The listed below is only in man-hours, to calculate the actual cost you have to multiply by the band rate of the person performing the activity. The estimation was done by SMEs and also from historical project data.

Table 3: Project Activity Estimation

Expense Category	**Security T and T (hours)**	**SSO BAU (Hours)**
Project Management	**1752**	
Analysis of the cybersecurity model definition	**1752**	
Identifying and modifying all supporting documentation, DOU, R&R/Security Solution Documents, Network, etc.		2000
Creation/modification of work instructions		2000
Training		200
Total	**3504**	**4200**

Source: Own work

Table 4: Human Resource Plan

Resource	**Description**
Overall project manager	• In charge of ensuring that the whole global project is completed successfully and within, time and within the expected benefit budget
Subproject manager	• In charge of subproject in a particular region • In charge of ensuring that the subproject is completed successfully within budget, time and within the expected benefit budget
Software development	• Making sure the right software, designs model used and in which particular area
Team Lead	• Work with teams to make sure work is done, trains the department members as well
IT SMEs	• Analyze and help in a specialized area and makes decisions for work to be smooth
Manufacturing Production leaders	• Help in the implementation in the manufacturing section
Legal service & support	• Help in the legal areas of the company

Source: Own Work

4.10.1 Risk management

Under risk Management the project should look at the following processes: -

- Risk mitigation: -This involves finding ways to reduce the impact of the risk transfer or avoid the risk from occurring.
- Transfer risks: - this involves transferring the risk to the department or organization that should deal with risk, especially if the risk is external
- Accept risks: -There are some risks whose impact and probably off occurrence is too low, these ones may be accepted.

Table 5: Overall risk and risk response

Short Risk/Issue definition incl. effect	***Prob. (%)***	***Impact L/M/H***	***Mitigation actions***
The volume of work instructions to be created is high and at the moment it is unknown	1	H	The two waves will be overlapping to ensure that work instructions created for wave 1 can be re-used for wave 2
Skills available to provide UID management across different platforms/applications may be difficult	0.5	H	To have few people with high Skill(2nd level) in the teams

to find and combine in a few individuals			
Lead time for hiring and training new employees is 2-5 months	0.5	H	Agreeing with the managers, whether employees will be moved with work or not
Risk of reduction of Quality of Service if the project is shortened	0.8	H	Planning has to be done carefully in order to ensure that the work is absorbed with BAU resources and quality of service is maintained.
Resource unavailability due to vacations and audit	0.9	H	Project Scheduling with the vacation periods in mind and also to ensure that as much work as possible is done before Summer vacations.
Security Department needs to be ready for the new work and the Management structure has to be in place	0.5	H	The two wave approach will ensure the management structure is set in the 1st wave and will be used in wave 2

Source: Own Work

- **Monitoring and controlling process Group**

  This consists of the process required to track and review the progress and performance of the project. Performance and progress have to be measured regularly. This is done in order to identify variances. Once the variances are discovered necessary changes need to be initiated and tracked.

It includes the following: -

- Monitoring the project activities against a baseline
- Monitoring changes and collective actions

The following processes in this group are the only relative.

- **Monitor and control project work**

This is the process of reviewing, approving, implementing and controlling and monitoring all change requests in the project. Need to follow the three steps

- **First, identify the change.** Be sure to clarify the scope of the change and well document it on ta change request form. Estimate the complexity and the cost of investigating the change. The steering committee will approve, reject or defer the change request.
- **Second, investigate the change.** This step might be performed by the steering committee. The change is investigated for its impact, as well as for the cost benefits of the change. Alternatives might need to be developed. The cost of the change request must be estimated and submitted to the steering committee.
- **Third, implement the change.** The change order provides instruction for implementing the change. Be sure to communicate impact assessment to stakeholders, including the originator of the change request.

- **Verify and control the scope**

Verifying scope is the process of formalizing the acceptance of deliverables. In this project, a checklist was used with the list of activities to ensure the activities of implementing g cybersecurity policy.

- **Control schedule and cost**

These two processes ensure that the cost and schedule baselines are maintained and can change that need to be approved.

- **Report performance**

The earned value was used to monitor project performance in order to make a decision on the project. **Earned value analysis** is the process of comparing, In terms of earned value, he projects actual performance against its planned performance. It can be calculated cumulatively or used to measure subprojects individually.

- **Monitor and control risk**

This is the process of continuously collect and analyses data about the identified risk to determine where action must be taken**.**

- **Closing process group**

  This process group contains the process necessary to close the project or phase of the project. The only process is relevant for this project in this group I is the close project or phase process.

Table 6: Closing Process Group Checklist

CUTOVER CRITERIA	PERSON RESPONSIBLE	STATUS
Approved and valid CBC covering service	Project manager	Yes
Approved and valid DOU covering service	DPE	Yes
Classification of Scope Type is still valid and approved PDR / Control Point	Sponsor	N/A
Transition Manager ensured that all transition activities took place. All stakeholders have been informed about the transfer, transfer phases and planned cutover to BAU date	Project manager	Yes
Accesses to customers systems granted	Project manager	Yes
All onboarding, compliance r requirements are known, documented, confirmed as possible to be fulfilled, and are fulfilled	Project manager	Yes
Tasks that are not allowed to be performed based on the contract are communicated	Subproject manager	Yes
Contractual Physical Security Requirements are implemented locally	DPE	Yes
All resources allocated signed a data privacy agreement	Project manager	Yes
The employee/employees allocated received complete Education/Knowledge Transfer needed to correctly perform the service	Project manager	Yes
BAU claim code is available and communicated	Project manager	N/A
Local Manager on Duty procedures verified against this particular transition and updated with specifics of this project requirements once applicable	DPE	Yes
The team is ready to perform the service in BAU mode	Project manager	Yes
Aftercare period conditions	Project manager	Yes
		100.00%

Source: Own work

Some closing activities to be completed

The major closing activity that was carried out where:

- Making sure the cutover checklist is at 100%

- Reviewing the agreement and project documentation to confirm that all, project deliverables have been met
- Formally closing the project with the sponsor and the suppliers
- Preparing a project evaluation report.
- Releasing staff and technical environments
- Gathering lesson learned and intellectual capital

5 CONCLUSIONS AND RECOMMENDATIONS

The aim of this thesis has been to identify the methods that are used to managing a global cybersecurity implementation project using PMI methodology in a manufacturing company. This has been achieved by conducting a semi-structured analysis some of the methodologies that companies over the years have adopted in implementing their projects. As presented in the previous chapters, the success of a company largely depends on the success of its projects. There is a growing interdependence between a firm's project and its survival in the competition.

The various aspect of the thesis has been put together to accomplish the objectives of the thesis.

Chapter one of this work was set to introduce the reader to the various elements and components of the thesis. The objectives of the studies, the significance of the study and the application boundary of this thesis were highlighted.

Next, a significant amount of literary work was reviewed, Current trend of cybersecurity issues as discussed by various authors and writers were discussed.

Chapter three of the thesis set to focus on some methodologies that manufacturing companies have adopted in the past and also presently. Advantages and disadvantages of using the methods were also discussed. The focused method PMI which happens to be the chosen method for this project was briefly introduced and continued from the next chapter.

Chapter four of this thesis dive deep into the chosen method, PMI for implementing cybersecurity program in a manufacturing company – Foxconn. A step by step approach through the entire implementation plan was discussed.

The project is now 90 percent finished and some of the benefits can be seen for example:-

- Mobile Device Management policy has been activated by 2nd of Dec
- Mass storage protection policy activated by 2nd of Dec
- Encryption is done
- Server rooms standardization
- Data share encryption
- Vulnerability/Penetration testing
- Network security controls switch patch level, all PC/NB in
- Annual education program - policy, threats, traveling, audits – training is in progress.

Thus to sum it all, Global cybersecurity project certainly saved purpose and increased the data protection In Foxconn and the benefits are justifiable.

been achieved by conducting analysis of implementing cybersecurity implementation in Foxconn manufacturing company.

5.1 RECOMMENDATIONS FOR FURTHER STUDIES

Understanding effectively and managing projects in a company is a key success factor of every company. Managers and project managers of companies are always looking for new and better ways of executing company projects. Even though the major focus of this thesis was on the PMI methodology for implementing cybersecurity project in a manufacturing company, other literature have it that, there are other success stories from other companies using other alternative methodologies to the PMI method discuss in this thesis. It is thus highly recommended that leaners and project managers who want to know more about how to select and adopt the appropriate methodology focus many studies on some other methods that may not have been fully discussed in this thesis.

This is to say, this thesis is not a conclusive write-up and judgmental work. It doesn't assign or endorses any PMI as the final and ultimate approach to all projects. It is therefore recommended that other methodologies be reviewed for proper and more insight into implementing cybersecurity programs the organization.

REFERENCES

[1] ABU-DOLEH, Jamal, & David Weir. "Dimensions of performance appraisal systems in Jordanian private and public organizations."*The International Journal of Human Resource Management.* 2007, 18(1), 75-84. ISSN: 0958-5192.

[2] ALEXANDER, Ian F., & Neil Maiden. *Scenarios, stories, use cases: through the systems development life-cycle*.2005.

[3] AL-HARBI, Kamal M. Al-Subhi. "Application of the AHP in project management." *International journal of project management.* 2001 19(1). 19-27.

[4] AMARATUNGA, Dilanthi, David Baldry, & Marjan Sarshar. "Process improvement through performance measurement: the balanced scorecard methodology."*Work study.* 2001, 50(5), 179-189. ISSN: 0043-8022.

[5] AMBLER, Scott W. "Agile model driven development is good enough." *IEEE Software* .2003.20(5). 71-73.

[6] AMBLER, Scott W. "The agile scaling model (ASM): adapting agile methods for complex environments." *Environments*. 2009. 1-35.

[7] AMBLER, Scott W. *The object primer: Agile model-driven development with UML 2.0.* Cambridge University Press, 2004.

[8] AVISON, David, & Guy Fitzgerald. *Information systems development: methodologies, techniques and tools*. McGraw Hill, 2002. pp. 608 ISBN: 978-0077096267.

[9] BALAJI, S., and M. Sundararajan Murugaiyan. "Waterfall vs. V-Model vs. Agile: A comparative study on SDLC." *International Journal of Information Technology and Business Management.* 2012. 2(1) .26-30.

[10] BURKE, Rory. "*Project management: planning and control techniques*." New Jersey, USA .2013.

[11] CADIEUX, Louise. "Succession in small and medium-sized family businesses: Toward a typology of predecessor roles during and after instatement of the successor."*Family Business Review*. 2007. 20(2).95-109.

[12] CAVELTY, M. D. Cyber-Terror Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate. *Journal of Information Technology & Politic.* 2008.4(1) 19-36.

[13] CHAPMAN, Chris, and Stephen Ward. *Project risk management: processes, techniques, and insights*. Wiley, 2003.

[14] CLARKE A Richard and Robert KNAKE . Cyber war: the next Threat to National security and what to do about. US: 2010. ISBN-10: 9780061962240

[15] COBURN, Andrew, Eireann Leverett, & Gordon Woo. *Solving Cyber Risk: Protecting Your Company and Society*. Wiley, 2018.

[16] COYLE, Robert G., & Robert Geoffrey Coyle. *Management system dynamics*. Vol. 6. Chichester: Wiley, 1977.

[17] ERICSSON, Göran N. "Cybersecurity and power system communication essential parts of a smart grid infrastructure." *IEEE Transactions on Power Delivery.*2010 . 25(3) 1501-1507.

[18] GIULIANI, A., A. Chen, S. Mereghetti, A. Pellizzoni, M. Tavani, and S. Vercellone. "Gamma-Ray emission from the Galaxy: a new model for AGILE." *Memorie della Societa Astronomica Italiana Supplementi.*2004. 5,135.

[19] HANSEN, Lene, and Helen Nissenbaum. "Digital disaster, cybersecurity, and the Copenhagen School." *International studies quarterly.* 2009. 53(4). 1155-1175.

[20] HARRIS, Mark, and Karen P. Patten. "Mobile device security considerations for small-and medium-sized enterprise business mobility."*Information Management & Computer Security*. 2014.22(1).97-114.

[21] HENDERSON-SELLERS, Brian, and Julian M. Edwards. "The object-oriented systems life cycle."*Communications of the ACM*. 1990.33(9).142-159.

[22] KOIKE, Hideki, Kazuhiro Ohno, and Kanba Koizumi. "Visualizing cyber attacks using IP matrix." In *IEEE Workshop on Visualization for Computer Security.* 2005.91-98. IEEE.

[23] KOSKELA, L. J., and Gregory Howell. "The underlying theory of project management is obsolete." In *Proceedings of the PMI Research Conference*. 2002. 293-302. PMI.

[24] LARSON, Erik W., and Clifford F. Gray. *Project management: The managerial process*. McGraw-Hill Education, 2017.

[25] LEE, Jay, Behrad Bagheri, and Chao Jin. "Introduction to cyber manufacturing."*Manufacturing Letters*. 2016. 8, 11-15.

[26] MCHUGH, Orla, and Mairéad Hogan. "Investigating the rationale for adopting an internationally-recognised project management methodology in Ireland: The view of the project manager." *International Journal of Project Management.* 2011. 29(5). 637-646.

[27] MUELLER, Frank. "Challenges for cyber-physical systems: Security, timing analysis and soft error protection." In *High-Confidence Software Platforms for Cyber-Physical Systems (HCSP-CPS) Workshop, Alexandria, Virginia,* p. 4. 2006.

[28] MOE, Nils Brede, Torgeir Dingsøyr, and Tore Dybå. "A teamwork model for understanding an agile team: A case study of a Scrum project." *Information and Software Technology*. 2010. 52(5).480-491.

[29] PROBST W Christian , Matt BISHOP & Dieter GOLLMANN. *is a cutting edge text presenting IT and non-IT facets of insider threats together*.US:Springer,2010.ISBN 9781441971333.

[30] PROJECT Management Institution. Guide to the project Management Body of Knowledge (PMBOK guide). US: New York, 2017.ISBN: 9781628251845.

[31] SADEGHI, Ahmad-Reza, Christian Wachsmann, and Michael Waidner. "Security and privacy challenges in industrial internet of things." In *2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)*. 2015 1-6. IEEE.

[32] SCHWABER, Ken. "Scrum development process." In *Business object design and implementation*. 1997. Springer, London, 117-134.

[33] SHAW, Eric D., Keven G. Ruby, and Jerrold M. Post. "The insider threat to information systems." *Security Awareness Bulletin*. 1998.2(98).1-10.

[34] ŠPUNDAK, Mario. "Mixed agile/traditional project management methodology–reality or illusion?."*Procedia-Social and Behavioral Sciences.* 2014. 119, 939-948.

[35] STEWAET James M, Mike CHAPPLE and Darril GIBSON. *overall information security program to protect organizations from growing sophisticate attacks*.US:Wiley,2015.ISBN 978111904271.

[36] TEIXEIRA, André, Saurabh Amin, Henrik Sandberg, Karl H. Johansson, and Shankar S. Sastry. "Cybersecurity analysis of state estimators in electric power systems." In *49th IEEE conference on decision and control (CDC)*. 2010. 5991-5998. IEEE.

[37] WEITZEL, John R., & Larry Kerschberg. "Developing knowledge-based systems: reorganizing the system development life cycle."*Communications of the ACM.*1989. 32(4) 482-489.

[38] WESTLAND, Jason.*The Project Management Life Cycle: A Complete Step-by-step Methodology for Initiating Planning Executing and Closing the Project*. Kogan Page Publishers, 2007.

[39] WONG, Joseph. "The adaptive developmental state in East Asia."*Journal of East Asian Studies*. 2004. 4(3).345-362.

[40] ZUR Muehlen, Michael, and Michael Rosemann. "Workflow-based process monitoring and controlling-technical and organizational issues." In *Proceedings of the 33rd Annual Hawaii International Conference on System Sciences*.2000. 10. IEEE.