Project Management: Changing the way Cyber Security works in an organization [1], [2]

Bhavyatta Bhardwaj

ABSTRACT

Cyber security forums and practices are at their peak with digital transformation of organizations all around the world. To address the issue of security, several models and frameworks have been developed and several practices have been introduced. These ideas need to be customised based on the business needs of the organization. A project management approach for cyber security is more comprehensive and effective for implementation of these practices. Unfortunately, the IT specialists and security gurus are not the only ones who log into the networks. A project manager can help the cyber security team to run projects smoothly within budget, and on time for completion, while ensuring security of the network and data. There can be a variety of recurring tasks or a major one-time task along with short-term and long-term priorities. A project manager can help run these responsibilities smoothly along with day-to-day functions of the team.

Keywords: cyber security, streamlined execution, strategic alignment, continuous improvement, business continuity, asset management, framework, models, practices, training

1. INTRODUCTION

According to John Chambers, Executive Chairman of Cisco System, “At least 40% of all businesses will die in the next 10 year, if they don’t figure out how to change their entire company to accommodate new technologies” [19] This is the truth of digital transformation. Information Technology (IT) has become widespread across every industry and is a backbone to business operations. Michelle Pruitt (Program Analyst at U.S. Department of Veterans Affairs) stated that project-based firms usually depend on system developers and project managers to ensure the security aspects of concerned projects. For a company to call itself a digital enterprise, it must implement profound changes such as making large investments in the latest technologies adopting new business models, modify existing models, using change management to train the organization for digitization, thereby attaining business continuity. Without considering security one may not consider an IT project as complete. A company should consider enhancing their IT infrastructure to improve its security posture and ensure reliable business operations. This paper explains how a project manager can help achieve these results

[1] Second Editions are previously published papers that have continued relevance in today’s project management world, or which were originally published in conference proceedings or in a language other than English. Original publication acknowledged; authors retain copyright. This paper was originally presented at the 13th Annual University of Texas at Dallas Project Management Symposium in May 2019. It is republished here with permission of the author and conference organizers.

[2] How to cite this paper: Bhardwaj, B. (2019). Project Management: Changing the way Cyber Security works in an organization; presented at the 13th Annual UT Dallas Project Management Symposium, Richardson, Texas, USA in May 2019; published in the *PM World Journal*, Vol. VIII, Issue IX, October.

for the company and describes a framework to clarify communication between the security team and development team. According to SysAdmin, Audit, Network and Security (SANS) Institute, security should be an input in communication planning [7] This paper will also explain how project management can help streamline security and compliance. As of 2017, 31% of organizations have experienced cyber attacks on operational technology infrastructure, according to Cisco [19] and cyber security venture projects damages related to cybercrime to hit $6 trillion annually by 2021 [19] Therefore, the main point of distinction for the success or failure of an IT project is the adoption of best security practices.

2. IT SECURITY, IT PROJCTS AND IT MANAGEMENT

According to IT governance, cyber security involves technologies, processes and controls designed to protect systems, network and data from cyber attacks. [18] A digital environment may also face major external threats unrelated to cyber environment, such as natural hazards, civil strife or terrorism. Any of these attacks may directly or indirectly impact an organization. Cyber security infrastructure includes devices and components to secure the digital environment and facilitate secure communication both within and outside of the organization. Organizations must ensure the digital security of assets that make it easy to control and overcome any cyber security issues to ensure that the organization is digitally secured.

In addition to securing the infrastructure, a company must also consider the specific security profile of the industry in which it operates. Upon the successful implementation and testing of a new and improved security profile, an organization may gain greater confidence in the level of protection it provides for its information assets [1]. Some of the factors that are likely to shift in the information security environment are [4]:

- New assets may be acquired.
- New vulnerabilities associated with the new or existing assets may emerge.
- Shift in business priorities.

Furthermore, a company must adopt a management model to manage and operate its ongoing security program [21] and regularly update it as needed. These management models consist of frameworks for managing a particular set of activities or business functions. For example, National Institute of Standards and Technology [10] identified has security frameworks that companies ay either use “as-is” or modify in congruence with the company’s compliance policies and standards. The security team can assist management and operation of the ongoing security program [3].

Every project has a beginning and an end. It will include a list of requirements, delivery schedule and maintenance plan that follows the management model. A project manager may be responsible to combine the specific requirements from corporate, operations and compliance teams for a successful security policy. The Project manager can help the cyber security team with its projects in the following ways:

1. **Streamlined project execution:** Client requirements and any concerns need to be communicated across the team. A project manager will make sure that the project has well defined milestones and deliverables.
2. **Strategic alignment:** Keeping in mind the company's goals and security principles, a project manager will protect the project against threats or risks while ensuring delivery and measurable return of investment (ROI).
3. **Optimized and Continuous resource allocation:** A project manager makes sure that resources are assigned in priority, and that the cyber security projects are executed efficiently, keeping in mind the resource capacity.
4. **Problem resolution:** A project manager provides an objective to the cyber security project and ensures that the potential problems are addressed and resolved appropriately and in a timely fashion.
5. **Risk management:** Project evaluation may depend on risks to decide whether the project should continue or not. Keeping that in mind, a project manager will lookout for all the additional risks that may come in way.

3. PROJECT SECURITY MILESTONES

Deliverables of security initiatives such as upgrades to network components will be audited by internal or external auditing consultants. By including security considerations in every phase of a project, project managers have the opportunity to deliver systems in a more secure manner.

The business case for an IT project should include strategic business goals whether the project delivers exciting new technology or a routine but essential upgrade to maintain enterprise productivity. IT project documentation also frequently includes sensitive details of the network and system architecture, which presents an attractive target for industrial espionage and hackers.

For every project, special attention to back ups, back out plans and security risks in early phases of project deployment will help the team to avoid overhead costs and delays. As project rollout leaves little time to consider how to undo the changes made during the go-live phase or react to an unexpected risk occurrence, it may cause systems to go down or cause data loss, corruption or breach.

Project managers should develop plans to mitigate such risks to project documentation and the methodology itself. A healthy security project management practice requires training and certification of the project team to promote awareness of security. It is recommended that developing and implementing an enterprise security plan be included in the IT governance model and communicated across the organization. This may include end-user computing guidelines to operating systems and network configuration.

The project manager is also responsible for becoming familiar with and complying with the policies of project sponsors. Ultimately, responsibility for implementation of these controls lies with technical teams. As project managers direct technical teams to accomplish project goals, they can leverage their awareness of critical controls and ensure their organization’s system has the most secure baseline configuration possible.

Following is a sample of a project security milestone plan: [4]

- IT Project
  - Initiate
    - Develop project charter
      - Security impact assessment completed
  - Planning
    - Develop project management plan
      - Security communication plan completed
  - Collect requirements
      - Security requirements collected
  - Execute
    - Develop project team
      - Security training completed
    - Operational Handoff
      - Security responsibility transferred
  - Closing
    - Security “Lessons learned” recorded

This plan may help, not only project managers, but also Chief Information Officers and Chief Information Security Officers, to streamline security policies with project deliverables by ensuring the data is secure from any cause of malicious attack, data loss, or breach while keeping systems up and running.

Finally, the financial impact of security needs to be determined before initiating any IT project. IT costs typically comprise a large portion of total cost for a project. On the other hand, failure to implement adequate security measures can be even more costly. Research shows average cost of recovery from a single security incident estimates to $86,500.00 for small and medium business and $861,000.00 for enterprises. [22]. Security measures require significant capital investment and project managers must analyze the costs to the project and to the company before investing in security [4]. All businesses cite IT infrastructure complexity as the key reason to invest in security, estimate 42-48% investments only for infrastructure security [22].

4. SECURITY ESSENTIALS FOR PROJECT MANAGERS

Confidentiality, Integrity and Availability, also known as the CIA triad, should be addressed in every project (Donn Parker, 1998). Project information protections, authenticity and timely accessibility are essential to reduce project risks. Project information consists of cost, scope, agreement information, staffing, communication channels and procurement.

The rapid growth in use of technology and the increase in connectivity between network environment and information systems have increased the chances of vulnerabilities and threats. Compliance with these standards ensures that the information is secured competently and also helps in reducing chances of project failure.

4.1 CIA Triad

The CIA Triad is a model that helps a company in applying its policies and security programs to protect their sensitive and confidential data. Depending on the sensitivity of data, IT projects may need to consider data confidentiality, whether they offer a new technology or existing one because they contain enormous knowledge of network and system architecture. Maintenance of CIA triads not only ensures the availability and integrity of data, but also strengthens the credibility and financial stability of companies who prioritize it [4]. A company is responsible for ensuring that all the three elements are addressed at all times.

4.2 Security program

A company should develop a security program that consists of policies, standards and guidelines. Policy is a high-level document that defines project objectives and standards that ensure compliance of policies. Standards are mandatory actions or rules to support and direct policies. Guidelines are recommendations designed to streamline certain processes according to best practices [23].

4.3 Risk management

Security value can only be truly justified when the risk is fully managed against the overall project cost and its maintenance

4.4 Team development

Developing teams and hiring the right people is a challenging task for IT managers because a poorly developed team can sabotage an effective project plan

4.5 Security awareness

Security should be considered from the beginning of the IT project to reduce possible chances of project failure

4.6 Access management

Project members’ access to the information, but also the system, premises and any project asset. Even though role-based access is important silos can sabotage the project

4.7 Business continuity and disaster recovery

In order to keep the project running smoothly, an IT project manager should also develop a business continuity plan [8]. In case of disaster, there should be a team who can respond to recover business operations quickly, while other members continue the support of necessary day to day activities like communication and administrative functions. This can be achieved by performing a business impact analysis, identifying resource values and determining project priorities and incident or crisis management plans [9]

4.8 Secure Documentation

A formal and secure document should be prepared to record all security requirements for the project, such as security management program (SMP) document. It is normally a collection of existing plans (i.e. risk management, work breakdown structure, assigned roles and responsibilities, project charter, scope and secure communication requirements) [5] The SMP document also contains security policies, standards, procedures, regulations and guidelines

4.9 Penetration Testing

Penetration testing should be performed, to evaluate how vulnerable a newly developed or existing system is and what impact it can cause on the entire project in case of vulnerabilities. To ensure the effectiveness of applied security controls, unit testing alone is not enough. The IT project manager must ensure performance of penetration testing [5] because it exploits the vulnerabilities to determine whether unauthorized access or other malicious activities are possible for the whole system, as opposed to the single module of unit testing.

5. INTEGRATION OF SYSTEM DEVELOPMENT LIFECYCLE (SDLC) WITH CIA TRIAD FRAMEWORK

According to NIST “Security assurance at each level of system development reduces risk of project failure and save all information assets of the project. The development lifecycle is a process that initiates with the development of a new project and ends with the disposal of the previously developed system or application” [10]

For example, plan schedule management utilizes inputs, tools and outputs. Using a framework that ensures confidentiality, integrity and availability ensures the security of the rest of the project, no matter which SDLC framework is being used for development.

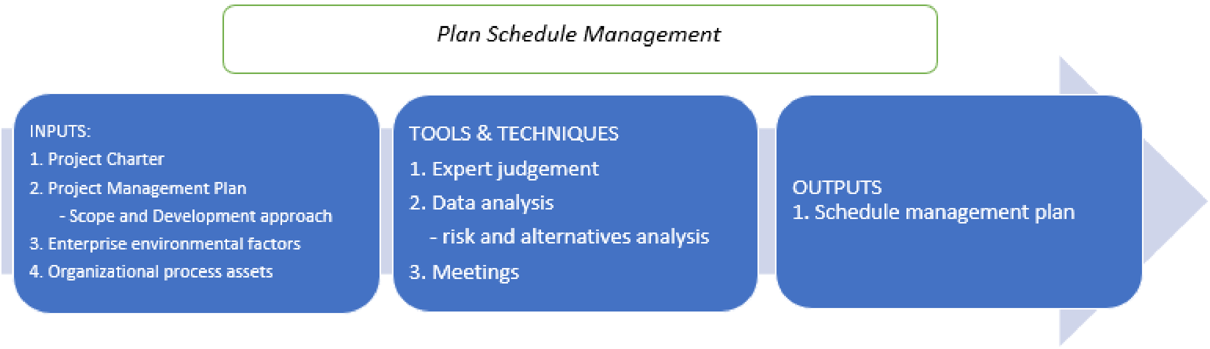
Plan Schedule Management
INPUTS:
1. Project Charter
2. Project Management Plan
- Scope and Development approach
3. Enterprise environmental factors
4. Organizational process assets
TOOLS & TECHNIQUES
1. Expert judgement
2. Data analysis
- risk and alternatives analysis
3. Meetings
OUTPUTS
1. Schedule management plan

Figure1: Plan schedule management [PMBOK]

Figure 1 is a sample plan schedule management model. The inputs to such a model from a security standpoint may include the security project charter, documentation, corporate policies and organizational security guidelines. The outputs produced by plan schedule management model may include security governance architecture to establish the policies as well as procedures and documentation for controlling a security project schedule.

In figure 2, the CIA triad is integrated with both agile and waterfall system development life cycles. It is a double purpose integrated framework that can be used by project managers to ensure that security is measured in every phase of system development and it can also be used by cyber security personnel to implement project management principles for cyber security projects. Each section has its own deliverable. Project managers can use these deliverables in meetings to communicate the concerns from security teams to development teams and vice versa. If a conflict arises, these deliverables, such as the security requirements, threat model, architecture and framework can be further discussed with the team. It is explained below for each phase in more detail:

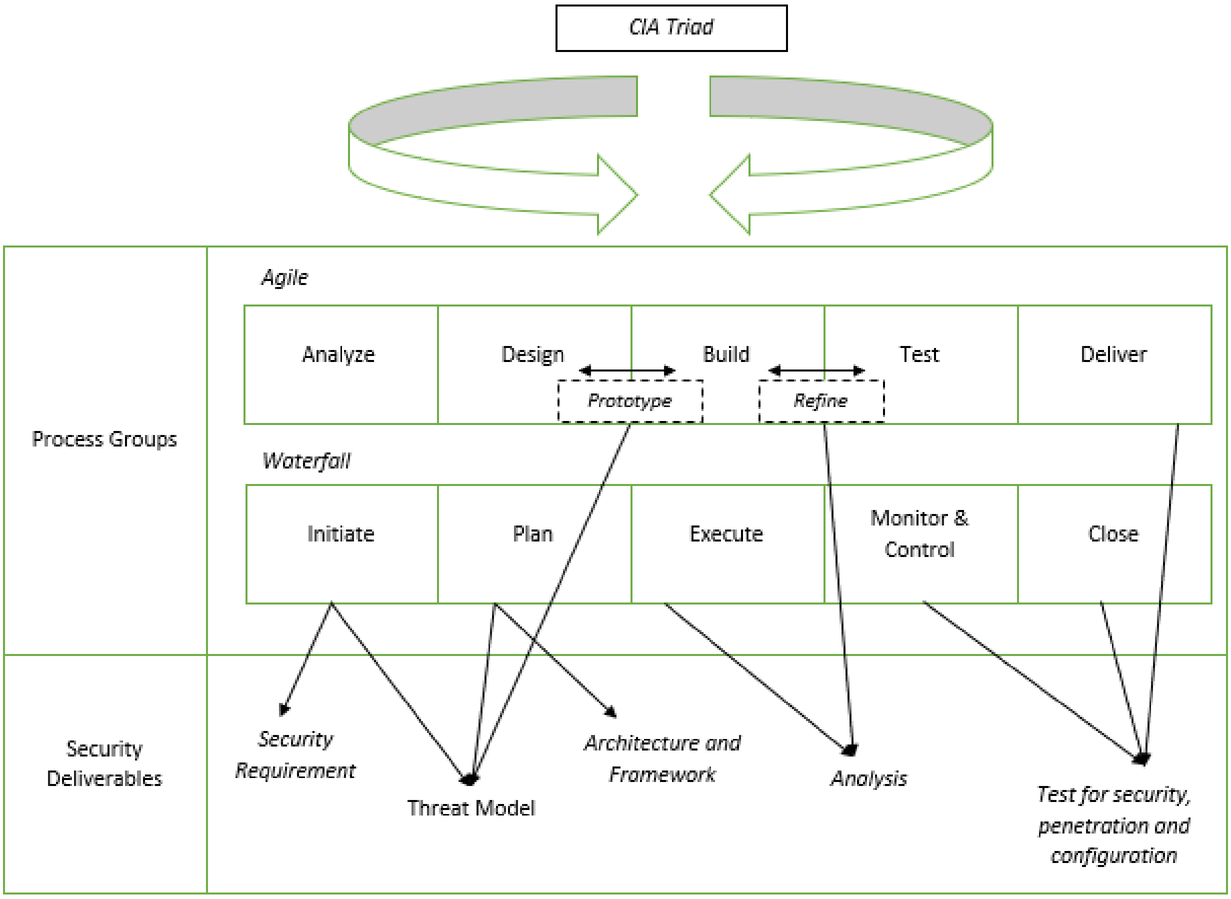

Figure 2: Integration of Security fundamentals with SDLC

Analyse/Initiate: in this phase an analyst can identify the problems and end solutions. A security program is developed, and feasibility studies are conducted. A project manager can align project objectives with security objectives.

Design/Plan: A project manager or analyst will determine security policies and guidelines that are in congruence with corporate policies. Business and/or user requirements can be gathered and documented. A list of all risks should be delivered in a threat model and plausible actions if the risk arises should also be documented and communicated throughout the team and stakeholders.

In case of an agile framework, the prototype must be refined as and when the security requirements are changed or enhanced to make sure every deliverable is secure and aligns with the CIA triad before it is delivered.

Build/Execute: A secure architecture and framework is created. It focuses on functional security requirement execution. A secure system is developed and tested to ensure that the system is error free. Vulnerability assessment should be conducted to find and fix any errors against the attacks.

Test/Monitor and Control: System integration must be completed in this phase and it should be tested against other systems for any flaws. Penetration testing is performed in order to refine the security measures and product specifications. This step also involves review and validation is all previously done work and its verification.

Deliver/Close: The system is delivered, and development is officially closed. The final documentation for training purposes must be delivered. For security purposes, back up of important data should be kept before the disposal of old system.

6. CONCLUSION & DISCUSSION

Project Managers should manage projects securely by applying security essentials into the project management process groups to ensure that the project is not only secure but also delivered on time, within budget and according to client specifications. The best time to address security is before any security risk or threat occurs, thus a project manager should develop a security program with the help of a security professional to reduce security risks as early as possible in the project lifecycle. This can be achieved by maintaining CIA at every phase of the project management process. Therefore, it is important to consider all aspects of security to reduce the probability of failure and overhead costs. This paper describes a framework with emphasis on security deliverables, which project managers may use to identify and communicate concerns across the entire team and stakeholders. A project manager can directly use this framework from initiation phase to close phase for streamlined execution of cyber security specific projects.

7. REFERENCES

1. A. Vance, M. Siponen, S. Pahnila, (2012) “Motivating IS security compliance: insights from habit and protection motivation theory”, Inf. Manage. 49, 2012, pp. 190–198.

2. A.C. Kim, S.M. Lee, D.H. Lee, (2012) “Compliance risk assessment measures of financial information security using system dynamics”, Int. J. Secur. Appl. 6, 2012, pp. 191–200.

3. Tripathi A, Singh UK. (2011) Taxonomic analysis of classification schemes in vulnerability databases. In: Computer sciences and convergence information technology (ICCIT), 6th international conference on. IEEE; 2011. p. 686–91.

4. Pruitt Michelle, “Security Best Practices” , (Online) “https://www.sans.org/reading-room/whitepapers/bestprac/security-practices-project-managers-34257”

5. S. Sangi, M. Ilkan, H. Tokgöz, “Incorporating Information Security in IT Project Management, School of Computing and Technology”

6. S.M. Soomro, T.R. and Brohi Ali, (2013) “Mapping Information Technology Infrastructure Library with other Information Technology Standards and Best Practices”, Computer Science.

7. SANS, (2013) "Security Best Practices for IT Project Managers", SANS reading room

8. Jiju (Jay) Nair, (2013) "Technology Project Management"

9. Albert Caballero, (2008) "Information Security Essentials for IT Managers: Protecting Mission Critical Systems", Terremark Worldwide, Inc.,

10. NIST, (2012) "National Institute of Standards and Technology Security Considerations in the System Development Lifecycle,"

11. Slideplay "Principles of Information Security" Chapter 12 https://slideplayer.com/slide/3001239/

12. M.N. Lakhoua, M.K. Jbira, (2012) "Project Management Phases of a SCADA System for Automation of Electrical Distribution Networks" IJCSI Vol 9, ISSN (Online): 1694-0814

13. Katharina Gerberding, " Benefits of project management for cyber security" (online-link) https://www.hitachi-systems-security.com/blog/5-benefits-of-project-management-for-cybersecurity

14. Andy Bochman, (2018) "The end of Cyber Security", https://hbr.org/product/the-end-of-cybersecurity/BG1803-PDF-ENG (Online)

15. F.A. Ali, M.Z. Ali, (2017) "Cyber Security Maintenance Based on Human-Technology Aspects in Digital Transformation Era" JESOC Vol 8, ISSN: 2289-1552

16. Jim Ditmore (2013), "Why Do Big IT Projects Fail so Often?".

17. Rajkumar, S. (2010). Art of communication in project management. Paper presented at PMI® Research Conference: Defining the Future of Project Management, Washington, DC. Newtown Square, PA: Project Management Institute.

18. https://www.itgovernance.co.uk/what-is-cybersecurity (Online)

19. https://cxo-transform.com/digital-transformation-quotes/ (Online)

20. https://cybersecurityventures.com/cybersecurity-almanac-2019/ (Online)

21. Guo, K.H, Yuan, Yufei (2012) "The effects of multilevel sanctions on information security violations: A mediating model" Information & Management, Elsevier Vol. 49, Issue 6, October 2012, Pages 320-326

22. https://www.kaspersky.com/blog/security_risks_report_financial_impact/ (Online)

23. https://frsecure.com/blog/differentiating-between-policies-standards-procedures-and-guidelines/ (Online)

About the Author

Bhavyatta Bhardwaj

Canada

🇨🇦 🇮🇳

Bhavyatta Bhardwaj is an early professional from Atlantic Canada with interest in Project management practices and cyber security. Previously with Bell Canada, she is now an IT consultant currently working for a utilities client. She has a Bachelor’s degree in IT from Uttar Pradesh Technical University in India and Master’s in Computer Science from University of New Brunswick in Canada. Bhavyatta specializes in optimal solution delivery for software development, implementation methodologies and frameworks, and IT operations management. She can be contacted at bhavyatta@gmail.com