ABS International Journal of Management
Volume XII Issue 2 December 2024 | ISSN 2319-684X (PRINT)

Cybersecurity Project Management Failures

Jay Barach
Vice President – IT Operations and Recruitment,
Systems Staffing Group, Inc. (Pennsylvania, USA)
ORCID ID: 0009-0009-0416-9712

ABSTRACT:
In the rapidly evolving landscape of cybersecurity, project management methodologies (PMMs) play a pivotal role in ensuring the success of cybersecurity initiatives. However, many organizations struggle with selecting the appropriate methodology, leading to project delays, budget overruns, and even failure. This paper investigates the causes and consequences of incorrect methodology selection in cybersecurity projects. Through an in-depth analysis of case studies, including real-world examples from sectors such as banking and healthcare, the paper highlights how inappropriate methodology choices, such as rigidly adhering to Waterfall or Agile, can result in ineffective security measures and project failure. Factors contributing to incorrect selection, including insufficient technical knowledge, unrealistic deadlines, budgetary constraints, and unclear project objectives, are explored. The paper further outlines recommendations for improving cybersecurity project outcomes by aligning project methodologies with organizational needs, focusing on stakeholder engagement, and incorporating continuous risk management practices. By offering guidelines on effective methodology selection, this research serves as a resource for project managers and cybersecurity professionals to navigate the complexities of cybersecurity project management and ensure better alignment between project goals and execution.

Keywords: *Cybersecurity project management; Methodology selection; Agile and Waterfall; Risk management; Project failure factors*

INTRODUCTION

As the world goes digital, cybersecurity continues to rise as a significant issue affecting organisations across different sectors (Culot et al., 2019). Ever more organisations use technology and data in their operations and thus experience more and diverse cyber threats, vulnerabilities which can lead to leakage of valuable data, to operational interruption, and to reputation loss (Culot et al., 2019). These risks can be managed through cybersecurity projects that put in place mechanisms of security like firewalls, encryption, access controls and intrusion detection (Culot et al., 2019). One thing that is clear today is that cybersecurity projects cannot be underestimated. Some of the potential costs of data breach are financial damage to an organization, legal consequences, and eroded customer confidence. Data from the IBM Cost of a Data Breach Report indicates that in 2021, the average cost per data breach was $4.24 million (Almulihi et al., 2022). Furthermore, it stated that the mean time to identify and respond to a cyber-attack was 287 days, suggesting the importance of preventive and efficient cybersecurity strategies (Almulihi et al., 2022). Cybersecurity projects are crucial for protecting an organization's assets which include data confidentiality, data and system integrity, and system availability (Goswami et al., 2023). They are useful for blocking intruders, identifying and counteracting security threats, and enhancing compliance with regulatory and legal requirements, including GDPR and PCI DSS (Goswami et al., 2023). The cybersecurity project entails more than technical know-how of the team but also the integration of efficient project management practices (Franco et al., 2022). Project management methodologies are frameworks that allow for planning, executing and controlling a project so that it can be delivered on time, within a given budget and to the necessary quality standards (Franco et al., 2022). Specifically, in cybersecurity projects, project management methodologies help to achieve objectives with the organisational security strategy, mitigate and manage risks and uncertainties, and facilitate project communication and cooperation among stakeholders (Blum & Blum, 2020). They assist in defining sub-goals, roles, and achievable objectives of large cybersecurity projects and monitoring the performance toward those goals. Various project management paradigms can be adopted for cybersecurity projects, and each paradigm has certain advantages and disadvantages (Goswami et al., 2023). Some of the popular models include Agile, Waterfall, Iterative Prototyping, DevSecOps, Lean Development, Spiral Model, FDD, XP

and Hybrid Model (Goswami et al., 2023). This is because the methodology depends on the complexity of the project, experience of a team, organizational culture, and security objectives. Although PMM is crucial in cybersecurity projects implementation, a lot of organizations face challenges when it comes to choosing the right methodology to implement. Issues arising from improper methodology choice include project delays, costs that are higher than anticipated, project expansion, and eventual project failure. When it comes to cybersecurity projects, the risks inherent to project failure might be considered higher since in such cases the organization remains exposed to cyber threats and the security of valuable information might be at stake. Consequently, this research paper seeks to examine how wrong choice of methodology influences cybersecurity project failures and proffer recommendations for how to prevent such failures. The paper, focusing on real-life cases, will show that inaccuracy in methodology choice is often the result of factors such as no technical experience, misunderstanding of management methodologies, cost, time, and unclear objectives.

Overview of Project Management Methodologies in Cybersecurity

When it comes to the implementation of cybersecurity projects, the choice of the right project management method and approach is not only essential for project success, risk management, and achievement of the set security goals but also critical for project success (Salin & Lundgren, 2022). Certain key updates of the recent times concerning project management can be depicted in this Table 1.

Statistic	Percentage
Projects that fail	70%
Companies undervaluing PM	42%
Budget overrun causing failure	55%
PM industry growth by 2020	$6.6 trillion
Successfully completed projects with supportive sponsors	62%
Wasted $ due to poor performance	9.9%
Increased success with PM practices	2.5x
Reduced waste with PM investment	28x
Lack of clear goals causing failure	37%
IT projects lacking confidence in success	75%
Lack of business-project alignment causing failure	44%
Construction projects underperforming	>50%
Underperformers citing inadequate sponsor support	41%
Organizations using PM software	22%
Organizations using standardized PM practices	93%
High performers using predictive approaches	44%
Productivity drop due to multitasking	40%
High performers with ongoing PM training	83%
PM-related roles needed by 2027	87.7 million
Projects meeting original goals	70%
Projects without effective sponsors	68%
Senior managers fully understanding PM importance	87%

Source: https://teamstage.io/project-management-statistics/

This section highlights nine main project management methodologies that are widely applied in cybersecurity projects and are also discussed in this work, namely Agile, Waterfall, Iterative Prototyping, DevSecOps, Lean Development, Spiral Model, Feature-Driven Development (FDD), Extreme Programming (XP), and Hybrid Methodologies. Both methodologies have their strengths and weaknesses that will be discussed in order to enhance understanding of the concept when selecting a method to adopt in the cybersecurity projects (Salin & Lundgren, 2022). Agile is a flexible project management methodology, especially useful in dynamic fields like cybersecurity, where rapid adaptation to emerging threats is vital. It promotes team collaboration, iterative progress, and customer feedback, using frameworks like Scrum and Kanban to break projects into short, manageable "sprints" (Chovanova et al., 2020). These sprints, typically lasting 2–4 weeks, allow cross-functional teams to develop working software increments that can be reviewed and refined based on feedback. Agile's major advantage in cybersecurity projects lies in its adaptability, enabling teams to address shifting priorities and new threats quickly, extending the project backlog to incorporate new security measures (Chovanova et al., 2020). Additionally, Agile fosters ongoing communication between stakeholders, ensuring security requirements are defined and tested throughout the project lifecycle. However, Agile's frequent feature changes can pose security risks if adequate security testing isn't consistently integrated (Chovanova et al., 2020). Moreover, its flexibility may become a limitation in highly regulated environments where strict compliance is required, making it challenging to

balance speed and security. The Waterfall methodology, in contrast, is a linear, phased approach that requires one phase to be completed before moving on to the next. It is suited for cybersecurity projects with stable, well-defined requirements where changes are minimal (Lieberum, 2023). The structured nature of Waterfall ensures thorough documentation and clear project timelines, making it easier to track and implement security requirements. This methodology is beneficial in environments that prioritize predictable planning and resource allocation (Lieberum, 2023). However, Waterfall's rigidity makes it difficult to respond to evolving security threats, as it lacks the flexibility to adapt to new security needs once the project is underway. Changes late in the project lifecycle, such as addressing security vulnerabilities discovered during testing, can be time-consuming and costly (Lieberum, 2023). This sequential model can slow down projects, especially in fast-paced cybersecurity environments where new threats emerge regularly, requiring a more iterative and responsive approach.

Table 2: Comparison of Project Management Methodologies in Cybersecurity

Methodology	Key Characteristics	Advantages	Disadvantages
Agile	- Iterative and incremental - Flexibility and adaptability - Collaboration and communication	- Rapid response to changing security needs - Early detection of security issues - Continuous improvement	- Potential neglect of comprehensive security testing and documentation - Challenges in highly regulated environments
Waterfall	- Linear and sequential - Well-defined phrases and deliverables - Emphasis on documentation	- Structured and disciplined approach - Clear tracking of security requirements - Better resource planning and allocation	- Inflexibility to accommodate changes - Costly and time-consuming to address security issues discovered later - Slow pace in rapidly evolving threat landscape
Iterative Prototyping	- Development and refinement of working prototype - Incremental building and testing - Regular feedback and improvement	- Early validation of security concepts and designs - Identification and mitigationof security risks - Stakeholder collaboration and alignment	- Potential neglect of comprehensive security documentation and testing - Difficulty in establishing a clear project timeline and budget
DevSecOps	- Integration of security into DevOps - Collaboration and automation - Continuous securitythroughout the lifecycle	- Accelerated delivery of secure software - Early identification and remediation of vulnerabilities - Culture of shared responsibility for security	- Requires significant organizational change and upskilling - Relies heavily on the quality and accuracy of automated security processes
Lean Development	- Maximizing value and minimizing waste - Continuous delivery of small improvements - Optimization of resource utilization	- Quick and incremental delivery of value - Faster feedback loops and adaptability - Culture of continuous improvement	- Potential neglect of comprehensive security testing and documentation - Challenges in applying lean principles to thorough security measures
Spiral Model	- Risk-driven approach - Combination of Waterfall and Iterative elements - Emphasis on risk management	- Proactive identification and mitigation of security risks - Incremental development and testing of security features - Stakeholder involvement and collaboration	- Requires thorough understanding and accurate assessment of security risks - May lead to longer project timeline and higher costs
Feature-Driven Development (FDD)	- Iterative and incremental - Focus on delivering working software features - Feature prioritization and tracking	- Quick and regular delivery of security features - Early validation of security controls - Clear communication and collaboration among team members	- Potential neglect of comprehensive security testing and documentation - May not adequately address holistic security needs
Extreme Programming (XP)	- Emphasis on simplicity, communication, and feedback - Short development cycles - Frequent delivery of working software	- Continuous security testing and validation - Close collaboration between developers and security experts - Early detection and resolution of security issues	- Potential neglect of comprehensive security documentation and formal processes - May not allow for in-depth security analysis and risk assessment
Hybrid Methodologies	- Combination of elements from different methodologies - Customized framework based on project needs - Adaptability to unique requirements and constraints	- Tailored approach to address specific security needs - Flexibility to adjust the approach as the project progresses - Leverages strengths of different methodologies	- Potential confusion and inconsistencies if not carefully planned - Difficulty in finding the right balance between practices and processes - Requires deep understanding and effective integration of component methodologies

Case Studies of Cybersecurity Project Failures due to Incorrect Methodology Selection

This section highlights three cases of cybersecurity projects that were either encountered with significant issues or were flat out failures due to the right decision of the project management methodology. For each case, the general context of the project will be disclosed; the details including the type of selected methodology, the rationale for its adoption, the result of the improper choice of the methodology, and the lessons learned from the case will be mentioned.

Case Study 1: Project Secure Data, ABC Bank Services

ABC Bank Services is a large international bank, and for the new

rules and regulations, it has implemented Project Secure Data to enhance the level of customers data. This project was aimed at solving the problems related to data encryption, access, and auditing of IT infrastructure of the organization that was in several facilities. The project duration was planned to take 18 months, and the total cost estimated was $10 million (Abidin et al., 2019). For Project Secure Data, ABC Bank Services selected the Waterfall methodology. Some of the reasons with the use of the Waterfall model included the perceived need for a significant amount of planning and documentation prior to the start of the project to meet the legal requirements, the desire for a linear approach to the project, and the comfort level or expertise of the development team with the Waterfall model. The organization thought that since Waterfall is a linear approach, it would present a logical and systematic framework through which the intended goals of the project can be met (Abidin et al., 2019). As working on Project Secure Data unfolded, several problems emerged because of the selected Waterfall model. The extensive documentation of requirements gathering phase took most of the overall project time and implementation and testing of security solutions were limited. Finally, when the implementation phase started the actual problems arose in terms of technicalities and compatibility that were not foreseen during the planning phase. Specifically, the Waterfall methodology was unable to respond to these challenges because of its highly structured approach. Scope and requirement changes are needed to undergo a change control process, making the project even more time-consuming and costly. Furthermore, the absence of continuous feedback and user participation in the process also contributed to the creation of security solutions that the organization might not necessarily require or wish to have. Towards the end of the project, the team was in a hurry to conduct the testing and deployment process, and therefore did not focus much on security testing, and even integrated many vulnerabilities into the production environment. The project was successful in terms of time and cost, but the result provided an inefficient security solution that could not satisfy all the regulations and the business goals.

1.In cybersecurity projects, the ability to be flexible and adaptable to changing specifications and threats is critical.

2.Some SDLC frameworks that support iterative and incremental development include Agile and DevSecOps, which allow for faster feedback, ongoing refinement, and adaptation to business requirements.

3. A central theme of this article is that over-reliance on planning and documentation in the early stages of the project can become a source of resistance to delivering value and adaptation.

4. Security solutions must be developed in consultation with the users and stakeholders for the whole duration of the project to address the organization's needs and concerns.

5. Allocating enough time and effort towards security testing and assurance activities for the security controls that are to be deployed is an important initiative.

Case Study 2: U.S. Department of Veterans Affairs (VA) - Scheduling Replacement Project

In FY 2000 VHA recommended the replacement of the scheduling system within VistA due to the age of the software. VHA began taking measures to shift from the system and the new Replacement Scheduling Application (RSA) development project was started with the help of COTS software program (Moldestad et al., 2021). The VA decided to implement the Waterfall-based model, which entails a linear process with well-defined stages, including requirement gathering, designing, implementation, and testing. The rationale for choosing Waterfall was due to the perceived size of the project, the formal documentation required, and the fact that the project team had prior experience with using Waterfall. During this project, some drawbacks resulted from the application of the chosen Waterfall methodology. The VA faced some difficulties due to the unclear definition and regulation of the requirements for the project, which caused the problems of scope creep and the delays. Since the Waterfall model mostly adopts a linear model, it was challenging to incorporate enhancement and users' feedback into the process (Dodaro & USGAO, 2019). Moreover, absence of iterative enhancement and testing also suggested that primary concerns were even more throughout the progress at the end stage and once again contributed to additional hours and dollars thrown away. One of the primary drawbacks of the project under analysis is its lack of flexibility and the failure to address new requirements and advancements in technologies. The failure of the VA's scheduling replacement project gave out so many lessons:

- Waterfall is less suitable in the case of large and complicated projects which require continual changes in the development process.
- Other paradigms, like iterative and incremental ones, including Agile methods, can provide quicker cycles of feedback, more extensive involvement of users, and flexibility to address dynamics of needs.
- Heavy documentation work at the beginning of the project and a linear approach to development might make it challenging for a project to adapt to changes and receive feedback from users.
- Regular testing and validation should not only be done on an exceptional basis, but rather at each stage of development to reduce possible challenges common in the later development stages of a project.

Case Study 3: Knight Capital Group - Software Deployment Failure

Knight Capital Group, a well-established American financial services firm, had embarked on a project to install an update to an automated trading platform in 2012. The project had the goal of increasing the performance and profitability of high-frequency financial transactions of the company (Min & Borch, 2022). The software deployment project at Knight Capital Group featured the use of an Agile method. The primary rationale for utilizing Agile was that the project required effort of high flexibility, fast results production, and fast reaction to the changes in the market. , as pointed out by Min and Borch (2022), the company expected Agile to be more flexible and therefore make it easier to release the software update while experiencing little disruption. However, the update that was released in August 2012 using the Agile methodology was a complete failure. The new software had a fatal error that initiated a chain of incorrect trades that resulted in a 45-minute $440 million loss (Min & Borch, 2022). Although Agile is all about being more flexible and delivering solutions as soon as possible, the improper approach to the methodology in question was one of the main reasons for the project's failure. The team worked towards speed and missed important components like testing, risk evaluation and configuration management. While Agile was thoroughly iterative, it failed to accommodate sufficient address to quality assurance and risk management. Furthermore, Edison et al. (2021) would note that the absence of effective governance, record-keeping, and reporting within the Agile environment aggravated the consequences of the software flaw. This fact shows that the team was primarily concerned with the timely release of the update and paid less attention to the stability of the system. The Knight Capital Group incident gave several lessons for software deployment projects using Agile methodology:

- Agile requires a balanced approach that combines flexibility with rigorous testing, quality assurance, and risk management practices.
- Rapid delivery should not compromise the need for thorough testing, especially in high-risk and mission-critical systems.
- Proper configuration management, version control, and documentation are essential, even within an Agile framework, to ensure system stability and facilitate issue resolution.
- Effective communication, collaboration, and oversight are crucial to identify and mitigate potential risks throughout the Agile development process.
- Continuous monitoring, real-time alerts, and rapid rollback mechanisms should be in place to minimize the impact of any issues that may arise during deployment.

Common Factors Contributing to Incorrect Methodology Selection

An appropriate project management methodology can lead to increased cybersecurity projects' success rates. As stated by Dobos and Csıszarık-kocsır (2022) it is crucial when managing projects in cybersecurity environment to choose an appropriate strategy for project management as well as aligning it to business initiatives effectively, as well managing projects' timely and efficient delivery. Nevertheless, organizations face difficulties when choosing the strategy because multiple factors affect their choices (El Khatib et al., 2022). This section discusses five significant sources of errors while selecting methodologies for cybersecurity activities and their impact on projects. The following are the challenges:

Insufficient technical knowledge and experience

The lack of technical skills and knowledge is another important factor that contributes to the improper choice of the methodology for a certain project in a team or in an organization (The role, 2022). Cyber security projects may include challenging technology, dynamic threats, and many other ideas

related to cybersecurity (Pollini et al., 2022). This implies that when the project managers or the decision-makers do not have adequate knowledge of these technicalities, then they might stumble when it comes to evaluating the applicability of various methodologies to the given project. From the case studies highlighted above, lack of technical knowledge as well as technical experience contributed to the choice of wrong methodologies. For instance, in the first case study, the adoption of the Waterfall methodology by ABC Bank Services was informed more by the fact that some members of the project team were already conversant with the approach than an assessment of how well the methodology suited the technical nature of the project. Likewise in Case Study 2, VA decided on the use of Waterfall despite the failure to consider the security implications which resulted in problems when incorporating the security practices. Due to the possibility of choosing an incorrect methodology due to the lack of technical knowledge, organizations must upgrade the knowledge and skills of their project teams. Enabling team members to develop and refresh their knowledge on cybersecurity technologies, processes, and trends with the current and potential methodologies of projects can improve decision-making capabilities (Pollini et al., 2022). Ramlo and Nicholas (2020) argue that security professionals working in the field and the subject matter experts should be involved in the selection of the most appropriate methodology.

Lack of knowledge of project management approaches

Another reason for selecting the wrong methodology is the lack of knowledge about project management methodologies and how they can be used in cybersecurity projects. According to the research done by Cremer et al. (2022), it is evident that any organizations lack adequate knowledge or understanding of the various methodologies that are being offered, the benefits of using such methodologies, or even the best way to apply such methodologies when it comes to cybersecurity activities Varela & Domingues (2022). These data are in line with insufficient understanding as one of the major reasons that cause people to select wrong methodologies in cybersecurity. From the case studies, the participants had limited knowledge of project management methodologies. For ABC Bank Services, choosing the Waterfall methodology as their model without any consideration of how this does not allow for changes in security needs was problematic for the following reasons. In Case Study 3 Knights' capital implementation of the Agile contract without appreciating how to incorporate security measures appropriately led to the emergence of security flaws and risks. To this end, there is a need for organizations to train their project managers and the teams on various available project management methodologies and the applicability of the methods to cybersecurity projects. This can be fostered through training programs, workshops, and certifications that are geared towards illustrating the application of project management in the context of cybersecurity as proposed by Cremer et al. (2022). This indicates that by increasing the understanding of the methodologies that are available and the suitability of each methodology for project types, organizations are in a better position to make the right choices.

Budgetary constraints

Lack of funds can also be a factor in choosing the wrong project management methodologies in cybersecurity projects. From Kerzner (2022)'s perspective, when organizations are cash-strapped, they may be inclined to opt for a method that seems to call for less money or fewer resources than another method, although it may be less appropriate for the project at hand. Budget limitations were never mentioned as a primary reason for choosing one or another methodology in the case studies. But it is important to understand that financial constraints can play a role in decision-making and may automatically result in compromising on the chosen methodology. For instance, an organization might choose the Waterfall approach to avoid what it perceives as the cost of iteration and constant security review, even though the Agile approach might better suit the requirements of the project in question. Therefore, organizations should tackle cybersecurity investment strategically to minimize the likelihood of choosing the wrong method due to inadequate funding. According to Kerzner (2022), this is accomplished by prioritizing the security plans based on their significance and risk and then apportioning resources. Costs and benefits of methodological selection allow organizations to make an accurate choice regarding an efficient and safe method based on strategic performance and economic aspects.

Unreasonable time expectations

Other causes that may result in the wrong adoption of project management methodologies in cybersecurity projects are unreasonable timelines and deadlines. As established by Bordley et

al. (2019), due to the desire to achieve results within a shorter amount of time, organizations can be tempted to use a method that gives the appearance of being quicker even where this methodology may not be ideal for the project in question. In Case Study 1, ABC Bank Services chose the Waterfall methodology because the company had to have a fixed time for the completion of the project. This decision caused project delays and the delivery of a less than optimum security solution. Likewise, in Case Study 2, VA's implementation of the Waterfall methodology without careful examination of the security testing and risks occurred because the company wanted to develop functional security features as soon as possible. To minimize the probability of choosing the wrong methodology due to tight or unrealistic timelines and deadlines, organizations should avoid adopting a rigid approach to project planning. According to Bordley et al. (2019), this entails realistic and effective goals, the project's sophistication level, and enough time for security testing and verification. However, the focus on quality and security over the speed of development means that the chosen methodology corresponds to project needs and allows delivery of high-quality and effective security solutions.

Ambiguity of the project's objectives and specifications

Another reason for choosing the wrong method in cybersecurity projects is the lack of clearly defined project goals and objectives. In a survey conducted by Varela & Domingues (2022) the experts identified risks in PM which include starting the project with wrong questions, project scope poorly outlined with the client. It is difficult to choose the right methodology suitable for the project if the objectives, deliverables, and success criteria are vague or if they are not communicated effectively. In the Case Studies, ambiguity pertaining to the project scope and requirements could be seen in Case Study 3, where Knight Capital implemented Agile Methodology without a clear understanding of security roles and responsibilities, which resulted in confusion and inconsistent implementation of security controls. Similarly, in Case Study 2, while VA set functional security goals and objectives, it did not have a strategic security plan and ended up with insecurely architected security controls. To mitigate this problem, organizations should devote adequate resources for the establishment of the project scope and requirements before embarking on any project. This involves consulting with stakeholders, broadly collecting requirements, and clearly defining project goals, outcomes, and measures of effectiveness (Varela & Domingues, 2022). Through defining and agreeing on the project objectives and deliverables, organization can identify the most suitable methodology to be applied in implementing the security controls to address the project requirements. As shown in the pie chart below, each factor is presented in proportion to its relative frequency of causing incorrect methodology selection across the case studies:

Ambiguity of the project's objectives and specifications

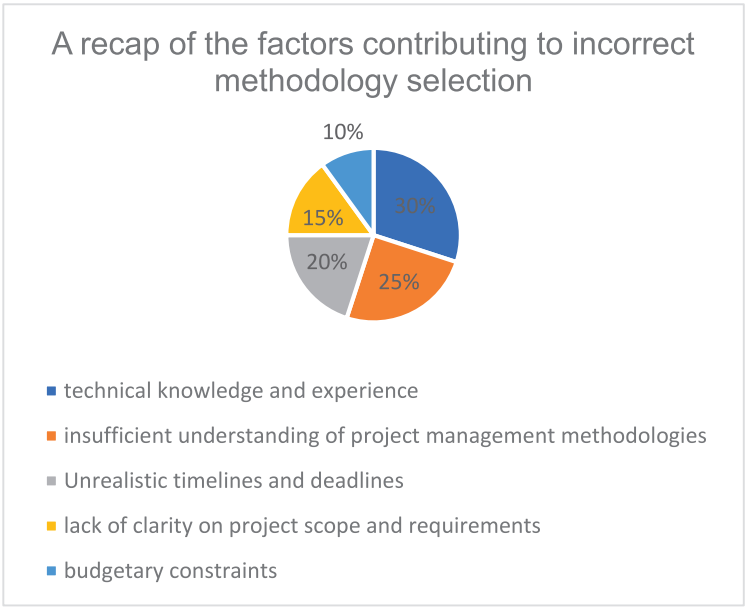

Figure : A recap of the factors that contribute to incorrect methodology selection in cybersecurity

Recommendations for Successful Cybersecurity Project Execution

Choosing the right project management methodology is a way to pave the path towards successful cybersecurity project delivery. However, the success of the project also depends on how properly the selected methodology is applied and maintained during the entire project cycle (Abrahams et al., 2024). This section will also include five best practices for cybersecurity project implementation together with their anticipated advantages and provide a table with these recommendations. After the best-suited methodology has been identified, sufficient training and support are required to enhance its application. Companies should engage in training activities that help the team members to develop relevant skills and knowledge pertaining to the selected approach. This training should include

information on the methodology: its aims and objectives, methods, instruments, and approach when used in the context of cybersecurity projects (Abrahams et al., 2024). Besides training, the organizational resources must be adequately provided to support the selected methodology. This entails availing the methodologies tools, technologies, and structures through which the team is able to implement the processes and practices of the given methodology (Abrahams et al., 2024). Another important aspect of adequate resources is that the required expertise is available for the team, for example, security specialists or experienced project managers who can help with the project implementation. Communication plays a vital role in the success of any project, and cyber security projects are not an exception. There is therefore a need for organizations to keep their members and stakeholders informed through clear and culture communication channels. These include formal or official meetings, briefings and progress reports to ensure that all stakeholders are informed and on the same page (Abrahams et al., 2024). Furthermore, organizations should promote communication in the organization, which allows employees to report issues, identify problems, and express possible solutions. Such an open culture can at times serve as an indication of possible mishaps and mitigate misconceptions and improve ownership of projects. Cybersecurity projects occur in complex and evolving environments which could be defined by ever evolving needs, goals, and threats. Therefore, it is necessary to revise the plans and schedules and their adaptation on a regular basis to remain focused on the project objectives and exclude possible divergence. This entails both the assessment of the project's situation, purposes, and deliverables to determine the ineffectiveness area or new reality that requires alteration (Abrahams et al., 2024). The planned reviews are also helpful to reflect on the suitability of the selected methodology and possibly contact some changes if needed. That is, organizations can keep project plans and timelines in check and avoid using too many resources while at the same time being aware of any deviation in the project's course. Any cybersecurity projects always come with certain risks that include data security breaches, system weaknesses, regulatory issues, and reputation loss. Hence, integrating risk management approaches that pertain to cybersecurity projects is imperative when it comes to project delivery. Managers should implement risk management protocols to identify, evaluate and prioritize the cybersecurity risks across the project lifecycle (Presley, 2022). This framework should be implemented into the chosen project management methodology to ensure that risk management activities are integrated with project processes and decisions. Managing risk in cybersecurity projects could entail security assessments, vulnerability scans, security control, and contingency and recovery plans (Presley, 2022). That is why managing cybersecurity risks means reducing the probability of security breaches and the consequences of such events in advance, thus ensuring the success of the project. To ensure cybersecurity project success, there needs to be a focus on improvement and growth. Members of the team working on a particular project need to be encouraged to experiment, innovate, and share knowledge with their colleagues. This culture should encourage best practice, the use of knowledge gained from other projects, and the ongoing improvement of team effectiveness (Presley, 2022). Some of the ways include daily or weekly meetings to reflect on the successes, challenges, and lessons learnt; or conducting retrospective meetings or post-project review meetings. They should be documented and applied to improve the management of the project and its processes for future projects. It is also important for organizations to provide regular training and professional development of their employees, so that they would be aware of the most recent developments and trends in cybersecurity (Presley, 2022). Hence, it would be possible to boost the organizations' abilities relating to the execution of projects, as well as to adapt to the changes that take place in the field of cybersecurity by promoting the culture of learning and improvement.

Table 3: Recommendations for Successful Cybersecurity Project Execution

Recommendation	Expected Benefits
Providing adequate training and resources for the selected methodology	- Enhanced team competency and efficiency in applying the methodology - Improved project performance and quality - Reduced risks of methodology misapplication
Establishing clear communication channels among team members and stakeholders	- Improved collaboration and information sharing - Early identification and resolution of issues - Increased stakeholder engagement and buy-in
Regularly reviewing and updating project plans and timelines	- Aligned project execution with objectives and changing circumstances - Effective resource allocation and risk mitigation - Timely identification and correction of deviations
Incorporating risk management strategies specific to cybersecurity projects	- Proactive identification and mitigation of cybersecurity risks - Enhanced security posture and regulatory compliance - Minimized impact of security incidents on project success
Embracing a culture of continuous improvement and learning	- Adoption of best practices and lessons learned - Continuous enhancement of team skills and capabilities - Improved adaptability to evolving cybersecurity landscape

The recommendations given can help to improve the outcomes of cybersecurity projects and to fully leverage the chosen project management approach in organizations. Thus, choosing the right methodology, applying it properly, and constantly adapting it is a way to ensure the successful implementation of cybersecurity solutions that meet certain organizational goals and reduce the risks of cyber threats.

Conclusion

In this research paper, the importance of choosing the right project management methodology for successful cybersecurity projects has been explored. Thus, we have described the aftermath of improper methodology selection and demonstrated how one should proceed to select the proper method. Cybersecurity initiatives are more often than not large-scale undertakings that must in the right sequence be designed, implemented, and managed. Selecting the right project management methodology plays a crucial role in achieving project goals and objectives, managing risks, and delivering effective solutions. Choosing the right methodology lays the groundwork for project planning, structuring, and management, as it correlates with certain parameters, limitations, and human resources. The analysis of case studies showed that the main issues leading to the incorrect selection of a methodology include lack of technical knowledge; inadequate knowledge of methodologies; budget constraints; unattainable time limits; and unclear definition of the project scope. To address these difficulties, guidelines for selecting a project management methodology include an analysis of the project needs, an evaluation of the team skills, the project size and level of risk, a determination of the level of flexibility required, the involvement of the stakeholders and the constant review of the methodology used. Support and proper management of the chosen methodology are necessary to achieve optimal results in the cybersecurity project. These are; proper training and resource provisions, proper communication channels, project plan review and update, incorporation of risk management and continuous improvement. Hence, this paper is a wake-up call for organizations to pay more attention to the choice of the right methodology in cybersecurity endeavours. Organizations need to spend considerable time and effort on identifying project needs, appraising team strengths and weaknesses, and determining the applicability of various approaches. In this way, by focusing on learning, improvement, and adaptation, organizations can improve their decision-making abilities to choose and deploy efficient methodologies enhancing their cybersecurity and safeguarding their resources from various threats.

References

- Abidin, M. A. Z., Nawawi, A., & Salin, A. S. A. P. (2019). Customer data security and theft: a Malaysian organization's experience. Information & Computer Security, 27(1), 81-100. https://doi.org/10.1108/ICS-04-2018-0043
- Abrahams, T. O., Ewuga, S. K., Dawodu, S. O., Adegbite, A. O., & Hassan, A. O. (2024). A REVIEW OF Cybersecurity Strategies In Modern Organizations: Examining The Evolution And Effectiveness Of Cybersecurity Measures For Data Protection. Computer Science & It Research Journal, 5(1), 1-25. http://dx.doi.org/10.51594/csitrj.v5i1.699
- Albuquerque, F., Torres, A. S., & Berssaneti, F. T. (2020). Lean product development and agile project management in the construction industry. Revista de Gestão, 27(2), 135-151. https://doi.org/10.1108/REGE-01-2019-0021
- Almulihi, A. H., Alassery, F., Khan, A. I., Shukla, S., Gupta, B. K., & Kumar, R. (2022). Analyzing the Implications of Healthcare Data Breaches through Computational Technique. Intelligent Automation & Soft Computing, 32(3). https://cdn.techscience.cn/ueditor/files/iasc/TSP_IASC-32-3/TSP_IASC_23460/TSP_IASC_23460.pdf

- Anjaria, D., & Kulkarni, M. (2021). Effective DevSecOps Implementation: A Systematic Literature Review. Revista Geintec-Gestao Inovacao E Tecnologias, 11(4), 4931-4945. ISSN: 2237-0722
- Anwer, F., Aftab, S., Waheed, U., & Muhammad, S. S. (2017). Agile software development models tdd, fdd, dsdm, and crystal methods: A survey. International journal of multidisciplinary sciences and engineering, 8(2), 1-10. https://www.ijmse.org/Volume8/Issue2/paper1.pdf
- Blum, D., & Blum, D. (2020). Strengthen security culture through communications and awareness programs. Rational Cybersecurity for Business: The Security Leaders' Guide to Business Alignment, 91-122. https://doi.org/10.1007/978-1-4842-5952-8_4
- Bordley, R. F., Keisler, J. M., & Logan, T. M. (2019). Managing projects with uncertain deadlines. European Journal of Operational Research, 274(1), 291-302. https://doi.org/10.1016/j.ejor.2018.09.036
- Camburn, B., Viswanathan, V., Linsey, J., Anderson, D., Jensen, D., Crawford, R., ... & Wood, K. (2017). Design prototyping methods: state of the art in strategies, techniques, and guidelines. Design Science, 3, e13. DOI: 10.1017/dsj.2017.10
- Chovanova, H. H., Husovic, R., Babcanova, D., & Makysova, H. (2020, November). Agile Project Management—What is It?. In 2020 18th International Conference on Emerging eLearning Technologies and Applications (ICETA) (pp. 167-175). IEEE. https://doi.org/10.1109/ICETA51985.2020.9379181
- Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: a systematic review of data availability. The Geneva papers on risk and insurance. Issues and practice, 47(3), 698–736. https://doi.org/10.1057/s41288-022-00266-6
- Culot, G., Fattori, F., Podrecca, M., & Sartor, M. (2019). Addressing industry 4.0 cybersecurity challenges. IEEE Engineering Management Review, 47(3), 79-86. https://doi.org/10.1109/EMR.2019.2927559
- Dobos, O., & Csıszarık-kocsır, A. (2022). The role of project management in cyber warfare with the support of artificial intelligence. The Eurasia Proceedings of Science Technology Engineering and Mathematics, 17, 26-37. https://doi.org/10.55549/epstem.1175898
- Dodaro, G. L., & United States Government Accountability Office. (2019). Veterans Affairs: Sustained Leadership Needed to Address High-Risk Issues. https://apps.dtic.mil/sti/citations/AD1166948
- Edison, H., Wang, X., & Conboy, K. (2021). Comparing methods for large-scale agile software development: A systematic literature review. IEEE Transactions on Software Engineering, 48(8), 2709-2731. Edison, H., Wang, X., & Conboy, K. (2021). Comparing methods for large-scale agile software development: A systematic literature review. IEEE Transactions on Software Engineering, 48(8), 2709-2731.
- El Khatib, M., Al Mulla, A., & Al Ketbi, W. (2022). The role of blockchain in e-governance and decision-making in project and program management. Advances in Internet of Things, 12(3), 88-109. https://doi.org/10.4236/ait.2022.123006
- Franco, M. F., Lacerda, F. M., & Stiller, B. (2022). A framework for the planning and management of cybersecurity projects in small and medium-sized enterprises. Revista de Gestão e Projetos, 13(3), 10-37. https://doi.org/10.5585/gep.v13i3.23083
- Goswami, S. S., Sarkar, S., Gupta, K. K., & Mondal, S. (2023). The role of cyber security in advancing sustainable digitalization: Opportunities and challenges. Journal of Decision Analytics and Intelligent Computing, 3(1), 270-285. http://dx.doi.org/10.31181/jdaic10018122023g

- Gubinelli, S., Cesarotti, V., & Introna, V. (2019). The evolution of project management (PM): how agile, lean and six Sigma are changing PM. The Journal of Modern Project Management, 7(3). DOI: 10.19255/JMPM02107
- Kerzner, H. (2022). Project management metrics, KPIs, and dashboards: a guide to measuring and monitoring project performance. John Wiley & sons.
- Kinyua, J. (2020). Cybersecurity in the software development life cycle. In Cybersecurity for Information Professionals (pp. 265-290). Auerbach Publications.
- Leong, J., May Yee, K., Baitsegi, O., Palanisamy, L., & Ramasamy, R. K. (2023). Hybrid project management between traditional software development lifecycle and agile based product development for future sustainability. Sustainability, 15(2), 1121. https://doi.org/10.3390/su15021121
- Lieberum, T. (2023). Behavioral Aspects in Project Management: A Comparison of Agile and Waterfall Project Management (Doctoral dissertation, Technische Universität München). https://nbn-resolving.de/urn/resolver.pl?urn:nbn:de:bvb:91-diss-20240622-1689900-0-0
- Macheque, V. (2019). Unbounded rule-based expert system for selecting software development methodologies (Doctoral dissertation). http://hdl.handle.net/11602/1305
- Min, B. H., & Borch, C. (2022). Systemic failures and organizational risk management in algorithmic trading: Normal accidents and high reliability in financial markets. Social Studies of Science, 52(2), 277-302. https://doi.org/10.1177/03063127211048515
- Moldestad, M., Stryczek, K. C., Haverhals, L., Kenney, R., Lee, M., Ball, S., ... & Young, J. (2021). Competing demands: scheduling challenges in being veteran-centric in the setting of health system initiatives to improve access. Military Medicine, 186(11-12), e1233-e1240. https://doi.org/10.1093/milmed/usaa520
- Pereira, T. S. (2019). Scrum and XP Agile practices used by project managers contribution towards software project success (Doctoral dissertation, Dublin Business School). https://esource.dbs.ie/server/api/core/bitstreams/4cbaf2f2-1311d-4e30-a124-21f1cf8c498d/content
- Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., & Guerri, D. (2022). Leveraging human factors in cybersecurity: an integrated methodological approach. Cognition, Technology & Work, 24(2), 371-390. https://doi.org/10.1007/s10111-021-00683-y
- Presley, S. S. (2022). Effective Cybersecurity Risk Management in Projects (Doctoral dissertation, University of South Alabama). https://www.proquest.com/openview/1ac0c6a6ec1a504a9024f6f24e6d774b/1?pq-origsite=gscholar&cbl=18750&diss=y
- Ramlo, S., & Nicholas, J. B. (2021). The human factor: Assessing individuals' perceptions related to cybersecurity. Information & Computer Security, 29(2), 350-364. ISSN: 2056-4961
- Salin, H., & Lundgren, M. (2022). Towards agile cybersecurity risk management for autonomous software engineering teams. Journal of Cybersecurity and Privacy, 2(2), 276-291. https://doi.org/10.3390/jcp2020015
- Varela, C., & Domingues, L. (2022). Risks of Data Science Projects-A Delphi Study. Procedia Computer Science, 196, 982-989. https://doi.org/10.1016/j.procs.2021.12.100