International Journal of Electrical Engineering and Intelligent Computing (IJEEIC) **EISSN 3031-5255**
https://ejournal.unkhair.ac.id/index.php/ijeeic/index

The Influence of Cybersecurity Practices on Project Management in Software Engineering

Shaymaa A. Chyad[1], Fırdews A. Alsalman[2], Esra Zuhair Majeed[3]
[1,2] Software Department, College of Computer Science and Mathematics, University of Mosul
[3] Sport sciences Branch, College of Physical Education and Sport Sciences, University of Mosul, Mosul, Iraq
[1]shaymaaahmedch@uomosul.edu.iq, [2] firdewsalsalman@uomosul.edu.iq, [3] esra.zuhair87@uomosul.edu.iq

Article history : Received August 8, 2026 | Revised August 26, 2026 | Accepted August 28, 2026

Cyber risks are gaining prevalence and complexity, which makes cybersecurity an essential aspect of software engineering project management. While this correlation is commonly accepted, little empirical evidence proves a relationship between cybersecurity measures and project management performance. This paper explores the relationship between five cybersecurity measures—secure coding, threat modeling, encryption and authentication, penetration testing, and continuous monitoring—and four aspects of project management, namely project timeline, project budget, team collaboration, and risk management. A quantitative survey research design was used in the study, which involved 128 software engineering experts and the application of multiple-response frequency analysis of organizational challenges and improvements in integrating cybersecurity into software engineering projects. The findings suggest that risk management preparedness, cybersecurity budgeting, and team collaboration are key dimensions related to the effective integration of cybersecurity into software engineering projects. Further results obtained through the application of the multiple-response approach revealed that lack of training, budget limitations, confusion about responsibilities, delayed cybersecurity measures, and ineffective cross-team collaboration are key organizational challenges preventing cybersecurity integration. Generally, the findings reveal that cybersecurity should be viewed as a strategic organizational capability rather than only a technical one. Practical suggestions concerning the integration of cybersecurity in SDLC are provided.

Keywords: Cybersecurity Practices, Cybersecurity integration, Project management effectiveness, Risk management, SDLC security, Software engineering.

1. INTRODUCTION

As the rate of technological change increases, connectivity of digital systems and the use of cloud computing is becoming the common business practice, and cybersecurity is a basic need in software engineering [1]. In addition to safeguarding software against cyber-attacks, cybersecurity has transformed into a strategic issue that has the potential to influence software quality, timely delivery, organizational resilience, and stakeholder trust. As a result, security has become a part of the Software Development Life Cycle (SDLC) instead of an activity executed at the end of software development life cycle [2].

Although organizations are becoming more aware of the importance of secure software development, they are still having challenges regarding how to incorporate cybersecurity into software engineering projects [5]. Challenges are especially faced are lack of skilled security personnel, lack of secure coding training, budget restraints, unclear roles, and changing requirements [4].

These become particularly important when we are talking about Agile and DevSecOps because of the short development cycles that require embedding security into the development process. The MOVEit Transfer event that happened in 2023 serves as a great example of how vulnerabilities in the deployed software can be exploited. The group CL0P used the vulnerability CVE-2023-34362, an unknown SQL-injection vulnerability in MOVEit Transfer, to hack into applications that were available on the Internet. They did so by using the LEMURLOOT web shell, thus obtaining access to the MOVEit Transfer databases and taking the data from it. There has been extensive research on technical cybersecurity practices, such as secure coding, software encryption, software authentication, threat modelling, penetration testing, and continuous monitoring, and most of the work has been conducted on how to enhance software protection by technical means [6].

On the contrary, few empirical studies have focused on the consequences of cybersecurity practices on software engineering project management. In particular, quantitative evidence that correlates cybersecurity with other project timeline, budget, team collaboration, and risk management is still limited. In response to this gap, the present study explores the relationship between the five cybersecurity practices and these four dimensions of project management via a mixed methods design that involves survey data for 128 software engineering professionals and multiple-response analysis of the open-ended items. It differs from previous research that focuses on cybersecurity technical mechanisms, since this research empirically proves that cybersecurity is a

strategic organizational capability that improves project performance. The results provide practical recommendations on how to embed cybersecurity in the SDLC for making projects more predictable, collaborative, risk manageable, and successful software engineering projects.

This research has four key contributions to the software engineering and cybersecurity literature. It offers empirical insights about the relationship between cybersecurity practices and software project management performance; examines the effects of cybersecurity practices on the project time, cost, teamwork and risk management; identifies the enablers and barriers to the integration of cybersecurity; and leverages an empirical example to show that cybersecurity should be considered as a project management practice rather than just a technical security measure for creation of software with security built in.

In the past decade, the approach toward a model of integrating cybersecurity and software engineering project management has evolved from a task-based model to an integrated, full life-cycle model approach. It has been discussed throughout the literature review as a part of software engineering and how it affects software engineering process development, and the critical role cybersecurity training and human factor aspects play.

The Software Development Lifecycle (SDLC) has evolved from a reactive to a proactive model and integrates Cyber Security to the whole software development lifecycle [8]. The SDL incorporates security practices into the development process, starting from requirement gathering to the maintenance after deployment in order to identify and mitigate the vulnerabilities from the outset [13]. The structured advice on secure software development can be found in secure software development frameworks such as OWASP Secure Coding Practices Checklist and CERT secure coding standards [19]. In addition, more methods like encryption, threat modeling, penetration testing, and the process of continuous monitoring can increase the security of the software being developed. Multiple benefits of AES are that it supports data confidentiality [10] and that in the secure-by-design approach, security is built into the software development process, not detected during operation [11]. Penetration testing and continuous security validation can help detect and mitigate emerging threats in a DevSecOps environment in a timely manner [14].

The five cybersecurity practices examined in this study—secure coding, threat modeling, encryption and authentication, penetration testing, and continuous monitoring—were selected to represent complementary security activities across major stages of the software development lifecycle. Threat modeling supports the identification of security risks during requirements and design; secure coding and encryption and authentication address security during implementation; penetration testing provides security validation; and continuous monitoring extends security oversight into deployment and operation. Together, these practices provide lifecycle-oriented coverage rather than focusing on a single stage of software development. Their selection is also consistent with established secure-development guidance emphasizing secure implementation, proactive risk identification, security validation, data and access protection, and ongoing monitoring [13], [20]. Importantly, each practice can also be examined in relation to the project-management dimensions considered in this study—timeline, budget, team collaboration, and risk management. The study therefore focuses on these five practices as a defined and manageable set of lifecycle-oriented cybersecurity activities rather than attempting to encompass the broader range of technical and organizational practices associated with DevSecOps.

Project management is a systematic process that uses knowledge, processes and techniques to meet the project's goals while managing cost, time, quality and risk [15]. A good plan, decision making and project tracking can be achieved in traditional and agile project environment with the help of frameworks like PMBOK Guide [16]. With the growing cyber security challenges, in software engineering, risk management has emerged as a critical success factor, even more important than cost [17]. Furthermore, efficient team cooperation and communication is important to connect with complicated tasks and enhance project overall performance [18].

By connecting the two fields in management, project management acts as a crucial intermediary for the organization's cyber protection and basic business procedures. Recent work argues that cybersecurity should be embedded across every project phase from initiation to closure, rather than treated as a late-stage technical activity [3], [20]. Security validation activities, including penetration testing, can consequently be incorporated at appropriate stages of the development lifecycle [12]. Previous work indicates that, project that adopt this model concerning the integration of the cybersecurity can lead to less post deployment security incidents, less expenditure to resolve issues as well as the gaining higher trust of the third parties stakeholders [21].

Although interest in cybersecurity within software engineering continues to grow, prior work exhibits several limitations that constrain what is currently known about its relationship with project management performance. Firstly, most of the previous works are theoretical papers or give frameworks and models for integration, but without empirical data to examine their findings. For instance, the latest papers on integration of cybersecurity into project management demonstrate descriptive rather than data-supported findings [3],[20]. Secondly, many of the previous works study cybersecurity from the technical point of view or analyze certain security practices in their isolation; thus, the research that they conducted does not provide the required insights on what impact cybersecurity has on software project management. Thirdly, at the moment there is a gap in literature concerning qualitative modeling that connects certain individual cybersecurity practices with measurable project management outcomes. Lastly, organizational aspect of cybersecurity integration, starting from early integration of SDLC and

ending with allocation of the budget and role definition, is not well represented in literature. In order to fill in these gaps, the current paper introduces quantitative survey-based methodology employing Likert scale and multiple response analysis that contributes to the body of knowledge about relationship between cybersecurity and software engineering project management.

2. METHODOLOGY

The authors conducted an inquiry using a quantitative survey-based methodology to evaluate the connection between cybersecurity practices and four factors of software project management—namely, timelines, budgeting, collaboration, and risk management. The data collection process was accomplished by means of a questionnaire made up of closed-ended five-point Likert-scale items along with multiple-response categorical items aimed at recognizing the ease of integration of cybersecurity measures. The questionnaire respondents were software developers, IT professionals, cybersecurity practitioners, and project managers who had at least one year of work experience in IT, finance, healthcare, and government sectors. To select sample members, purposeful sampling was employed to make sure that they all possess relevant experience. Out of 160 questionnaires sent out, the research obtained 128 responses fitting the criteria for analysis which constituted a response rate of 80.0%. Despite the studies being conducted with the help of purposive sampling, the lack of randomness in sample selection might result in biased results. Though the response rate is high enough, some other bias because of non-responses might occur. The required sample size was found to be within the acceptable limits, according to G*Power analysis..

The structure of the questionnaire consists of three major sections, including demographic and professional information; 10 five-point Likert scale questions designed to measure cybersecurity practice in four areas of project management namely timeline, budget, teamwork, and risk management; and two multiple-choice items (Q11 and Q12) where participants could select any of the possible answers available concerning the problems and solutions of cybersecurity integration respectively. The demographics of the respondents can be found in Table 1 and the survey items in Table 2. The questionnaire was subjected to scrutiny by experts in the field for its clarity and reliability. The items Q11 and Q12 were evaluated via frequency analysis on multiple-choice questions as they required predefined answers.

Table 1: Participant Demographics

Working Area	Frequency	Education	Persons
Software Development	72	Bachelor's Degree	88
IT Services & Support	34	Master's Degree	32
Academia	12	Doctoral Degree	8
Government Sector	10	Experience	
Sex		1–5 years	46
Male	84	6–10 years	38
Female	44	>10 years	44

The survey items and corresponding project management dimensions are summarized in Table 2. The questionnaire included ten five-point Likert-scale items addressing project timeline, budget performance, team collaboration, and risk management, together with two multiple-response questions addressing challenges to cybersecurity integration and strategies for improvement. These items were designed to capture participants' views on the relationship between key cybersecurity practices and software project management. The following were selected to elicit participants' views on the impact of critical cybersecurity activities on software project management, as well as issues and solutions for further integration of cybersecurity.

Table 2: Survey Questions

Section	Questions
Impact on Project Timeline	Q1. Implementing cybersecurity secure coding standards during development tends to delay project deadlines.
Likert Scale (1–5)	Q2. The integration of cybersecurity threat modeling in the early stages of a project improves adherence to project timelines.
Budget Influence	Q3. Cybersecurity encryption and authentication security also add to the overall cost of the project.
Likert Scale (1–5)	Q4. The funding that might be expended on cybersecurity and encryption, as well as authentication, is recouped due to the long-term savings (such as preventing breach).
Team Collaboration	Q5. Cybersecurity penetration testing requirements improve collaboration between project management and development teams.
Likert Scale (1–5)	Q6. Project teams often struggle to balance cybersecurity penetration testing requirements with other project goals (e.g., speed, innovation).
Risk Management	Q7. Cybersecurity monitoring and frequent security updates can help control project risks such as data breaches or system disruptions.
Likert Scale (1–5)	Q8. Project managers are well-suited to handle exposure of cybersecurity, ongoing monitoring, and security updates.

	Q9. Software project planning stages. Software project planning phases often overlook cybersecurity threat modelling factors.
	Q10. All project personnel should have cybersecurity training and awareness programs on all practices.
Multiple-Response	Q11. What are the most significant challenges your team has encountered in applying particular cybersecurity practices to project management?
Multiple-Response	Q12. Based on your experience, how could the inclusion of cybersecurity practices into project management be enhanced?

Consistent with the survey instrument, in which individual items capture perceptions of cybersecurity practices in relation to specific project-management dimensions, the statistical analysis focuses on four measured constructs: project timeline, budget influence, team collaboration, and risk management preparedness. As illustrated in Figure 1, the five cybersecurity practices—secure coding, threat modeling, encryption and authentication, penetration testing, and continuous monitoring—provide the conceptual foundation for the survey items but were not operationalized as separate independent predictor scales. Accordingly, the correlation and regression analyses examine relationships among the four project-management dimensions rather than estimating the independent effect of each cybersecurity practice.

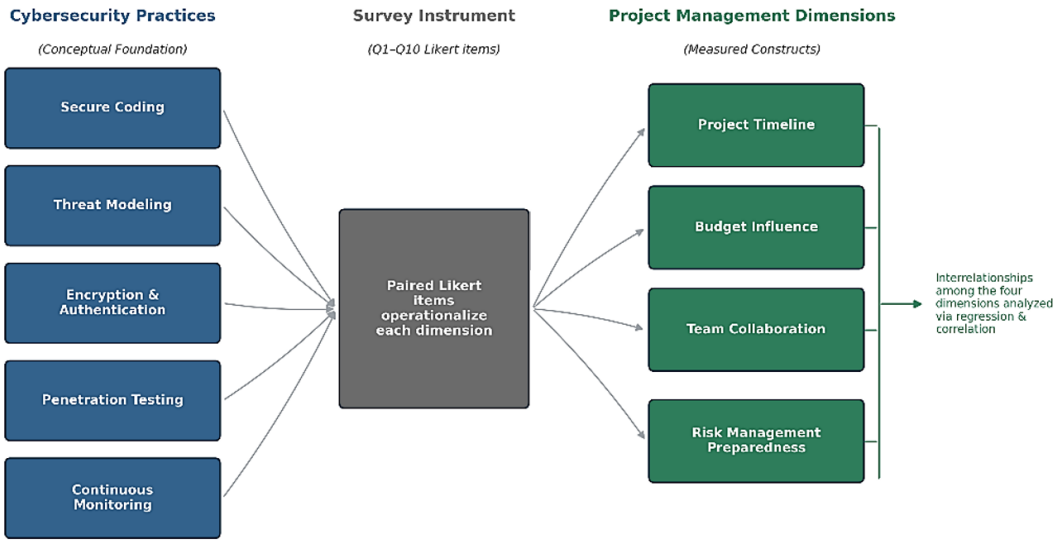

Figure 1. Analytical framework linking cybersecurity practices, the survey instrument, and the four measured project-management dimensions

Definitions and measurement description of the variables: definitions and measurements for each variable are presented in Table 3.

Table 3: Mapping of Variables and Survey Items

Variable Type	Variable	Survey Questions	Project Management Dimension
Conceptual Cybersecurity Practice	Secure Coding	Q1, Q2	Timeline
	Threat Modeling	Q2, Q7	Risk mitigation, Budget performance
	Encryption & Authentication	Q3, Q4, Q7	Budget performance, Risk mitigation
	Penetration Testing	Q5, Q6, Q7	Team collaboration, Risk mitigation
	Continuous Monitoring & Security Updates	Q7, Q8, Q10	Risk mitigation, Team collaboration
Measured Project Management Dimension	Impact on Project Timeline	Q1, Q2	—
	Budget Influence	Q3, Q4	—
	Team Collaboration	Q5, Q6	—
	Risk Management	Q7, Q8, Q9, Q10	—
Multiple-Response (Categorical)	Implementation challenges	Q11	—
	Improvement strategies	Q12	—

Note: Cybersecurity practices are mapped to survey items to indicate the conceptual basis of the questionnaire and were not operationalized as separate independent predictor scales. Statistical analyses were conducted at the level of the four measured project management dimensions. Q11 and Q12 were multiple-response categorical items analyzed separately using frequencies and percentages.

The overall Cronbach's alpha of the questionnaire was 0.832, indicating good internal consistency. IBM SPSS was used for statistical analysis, including descriptive statistics, Pearson correlation, and multiple linear regression. The responses to questions Q11 and Q12 were analyzed using multiple response frequency analysis. This method was chosen because each respondent was able to choose multiple options from the list generated by the researchers. As each response category was treated separately from the others, this process does not allow for qualitative coding and determining inter-coder reliability and using qualitative data analysis software. The findings from the multiple response approach were used in conjunction with the quantitative findings to interpret the results of the research.

3. RESULTS AND DISCUSSION

In this section the quantitative and qualitative results regarding the link between cybersecurity practices and software engineering project management are presented. The results are presented using descriptive statistics, regression and correlation analyses, hypothesis testing, and multiple-response frequency analysis. 1.

3.1 Descriptive Analysis

Descriptive statistics were employed to present the answers provided by the participants in the four main dimensions of the project management: project time, influence of budget, team cooperation, and readiness for risk management. The mean value for all dimensions was above 3.50, as presented in Table 4, suggesting overall positive perceptions in cybersecurity practices and software engineering project management.

Table 4: Descriptive Statistics

Variable *	Mean	Standard deviations (SD)	Explanation
Project Timeline	3.52	0.73	This metric shows how participants view cybersecurity practices impacting the project delivery timeline. The moderate mean indicates that while several respondents believe that cybersecurity can cause delays to project timelines, this does not seem to be viewed as a large source of disruption across all projects by the respondents.
Budget Influence	3.91	0.90	There is a common perception that integrating cybersecurity into projects increases the overall cost. Similarly, with an average response we can infer that respondents strongly believe that cybersecurity does increase the overall cost of a project, however the higher than average standard deviation suggests some variance in perception and in meaning.
Team Collaboration	3.64	0.79	The extent to which cybersecurity requirements can help or hinder collaboration among project managers, developers and security experts is also tested in this paper by using a mean score. Since an increased average score implies that a larger majority of the respondents strongly agree or disagree that cybersecurity has a positive or adverse effect on their collaboration activities.
Risk Management Preparedness	3.71	0.67	This specifically measures how well project teams are handling cyber-risks (such as breaches or compliance). A notorious average with minimum standard deviation means of all projects recognize that cybersecurity helps in efficiently controlling their risks.

The highest mean (M = 3.91) was for budget influence, followed by risk management preparedness (M = 3.71), team collaboration (M = 3.64), and project timeline (M = 3.52). The standard deviations was between 0.67 to 0.90, suggesting that responses were fairly consistent across the four factors.

3.2 Regression Analysis

Four multiple linear regression models were created for exploring the connections among the four dimensions of project management that were measured. Depending on the structure of the models shown in Table 5, the timeline of the project, the effect of the budget, the collaborative work of the team, and the readiness towards risk management were taken sometimes as dependent variables, and sometimes as independent variables. The analyzation in question shows the relationships between the considered dimensions, although it does not give information about the influence of separate measures related to cybersecurity.

Table 5. Regression Models for Assessing Interrelationships Among Project-Management Dimensions

Model	Outcome Variable	Predictor Variables
1	Project Timeline	Budget Influence, Team Collaboration, Risk Management Preparedness
2	Budget Influence	Team Collaboration, Risk Management Preparedness
3	Team Collaboration	Budget Influence, Risk Management Preparedness
4	Risk Management Preparedness	Project Timeline, Budget Influence, Team Collaboration

3.3 Correlations Analysis Results

The Pearson test was conducted using the most critical variables of project management, which were time to schedule, budget impacts, team integration, and readiness of the teams to manage the risks. Table 6 elaborates on these results as well as on other project management variables.

Table 6: Pearson Correlation Matrix

Variables	Project Timeline	Budget Influence	Team Collaboration	Risk Management
Project Timeline	1			
Budget Influence	0.597	1		
Team Collaboration	0.510	0.481	1	
Risk Management	0.645	0.606	0.563	1

Table 6 displays the Pearson correlations among four project management dimensions that have been studied. All dimensions are positively and significantly correlated ($p < 0.01$). The highest relationship is between project timeline and risk management preparedness ($r = 0.645$), followed by budget and risk management preparedness ($r = 0.606$). Additionally, team dynamics shows a positive correlation with risk management preparedness ($r = 0.563$). These results reflect significant relationships between different dimensions of project management in cyber security integration and especially high correlations of risk management preparedness with budget and timeline. The relationships can be viewed in Figure 1, illustrated in the correlation heat map.

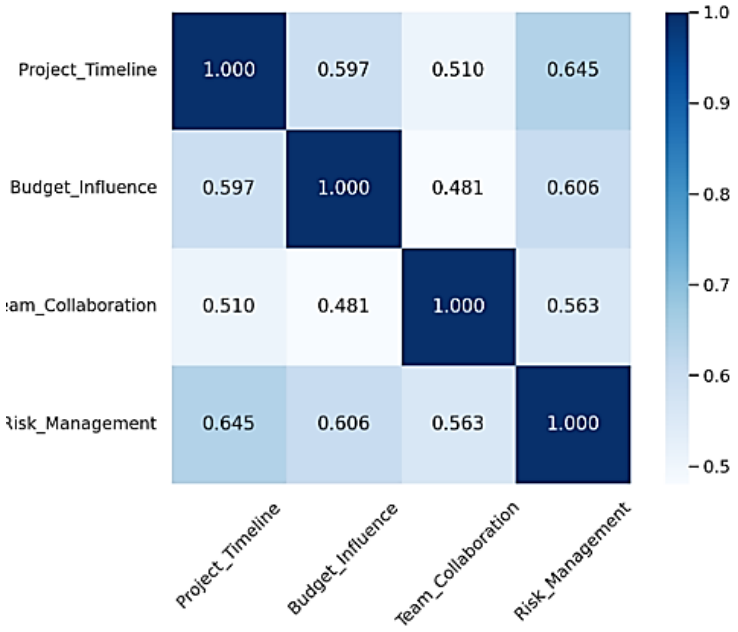

Figure 2. Pearson Correlation Matrix Showing Relationships Between Project Timeline, Budget Influence, Team Collaboration, and Risk Management

3.4 Results for Hypothesis Testing

The four a priori hypotheses were tested by means of regression analysis as outlined above. The results of testing each hypothesis are described in Table 7 below, along with an explanation.

Table 7: Hypothesis Testing for Relationships Among Project-Management Dimensions

Hypothesis (H)	Research Question (RQ)	Statistical Test(s)	Outcome
H_1 – Budget influence, team collaboration, and risk management preparedness are significantly associated with project timeline	RQ1	Multiple regression (Model 1). $R^2 = 0.499$, $F(3,124) = 41.21$, $p < 0.001$. Significant predictors: Risk Management $\beta = 0.381$ ($p < 0.001$); Budget Influence $\beta = 0.292$ ($p = 0.001$); Team Collaboration $\beta = 0.156$ ($p = 0.050$).	Supported
H_2 – Team collaboration and risk management preparedness are significantly associated with budget influence	RQ1	Multiple regression (Model 2). $R^2 = 0.396$, $F(2,125) = 40.95$, $p < 0.001$. Predictors: Risk Management $\beta = 0.491$ ($p < 0.001$); Team Collaboration $\beta = 0.205$ ($p = 0.016$).	Supported
H_3 – Budget influence and risk management preparedness are significantly associated with team collaboration	RQ2	Multiple regression (Model 3). $R^2 = 0.348$, $F(2,125) = 33.30$, $p < 0.001$. Predictors: Risk Management $\beta = 0.429$ ($p < 0.001$); Budget Influence $\beta = 0.221$ ($p = 0.016$).	Supported
H_4 – Project timeline, budget influence, and team collaboration are significantly associated with risk management preparedness	RQ2	Multiple regression (Model 4). $R^2 = 0.535$, $F(3,124) = 47.59$, $p < 0.001$. Predictors: Project Timeline $\beta = 0.353$ ($p < 0.001$); Budget Influence $\beta = 0.274$ ($p = 0.001$); Team Collaboration $\beta = 0.250$ ($p = 0.001$).	Supported

3.5. Interpretation of the Hypotheses:

The regression analyses supported all four hypotheses and demonstrated significant interrelationships among the measured project-management dimensions. Risk management preparedness showed particularly strong associations across the models, including with project timeline, budget influence, and team collaboration. These findings suggest that the project-management dimensions associated with cybersecurity integration are interrelated rather than operating independently. In particular, stronger risk management preparedness is associated with more favorable perceptions of timeline management, budgeting, and team collaboration within software engineering projects. In conclusion, it can be seen from the results obtained that effective cybersecurity practices make software engineering project management more effective. It can also be said that the main parameters contributing to project effectiveness are risk management establishment, correct allocation of cybersecurity, timely introduction of security measures and collaboration of the members of the project team. These practices, when implemented together, result in better project predictability, more efficient use of resources, increased organizational agility and effectiveness, and better software engineering projects. The results prove that the issue of cyber security needs to be treated as a strategic organizational competency and not just a security technical activity. To complement the quantitative analysis, the two open-ended survey questions, which both were answered by the same 128 software practitioners, were analyzed using multiple-response frequency analysis. Five predefined challenge categories were most frequently selected by respondents, cybersecurity integration were identified and their frequencies with associated responses are summarized in Table 8.

Table 8: Integration Challenges

Category	Definition	Frequency (n)	Example Response
Limited Team Training / Awareness	Inadequate or irregular cybersecurity education for project staff.	67	“Most team members lack up-to-date security knowledge.”
Budget Constraints	Insufficient or non-ring-fenced funds for cybersecurity activities.	59	“Security is always the first item cut when budgets tighten.”
Unclear Roles & Responsibilities	Ambiguity about who owns, executes, or signs off on security tasks.	50	“No one knows who is accountable for vulnerability fixes.”
Late Integration of Cyber-Security	Security considerations were introduced after major design/coding phases.	47	“We addressed security only in the final sprint, causing rework.”
Poor Cross-Team Collaboration	Siloed working and limited communication between PM, dev, and security teams.	43	“Developers and security staff rarely meet; issues slip through.”

Qualitative analysis revealed the following key organizational challenges to implementing cybersecurity: training, budget constraints, unclear role responsibilities, late cybersecurity integration, and limited team collaboration. The results of this finding are in line with the quantitative findings and support the conclusion that organizational factors are critical in managing software engineering projects. Together, these findings highlight the need for ongoing training, proper budget planning, role definition and early inclusion of cybersecurity in projects. The frequency of these categories is summarized in Figure 3.

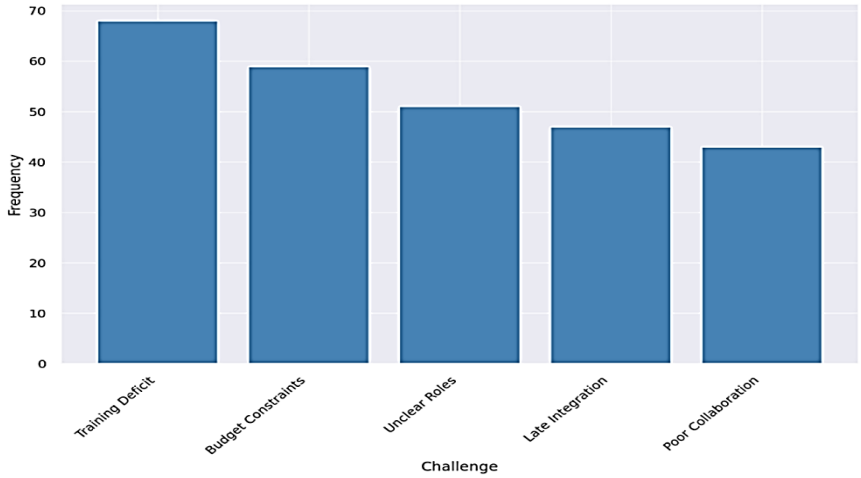

Figure 3. Cybersecurity Challenges

Open responses with suggestions on improving cybersecurity integration corresponded to five predefined improvement-strategy categories. The frequency and representative comments for these categories can be found in Table 9.

Table 9: Improvement Strategies

Category	Description	Frequency (n)	Example Response
Provide Regular Training	Ongoing, role-specific security awareness and skills programs.	74	"Continuous cybersecurity training must be mandatory for all team members."
Involve Security Experts Early	Embed security professionals during planning / requirements phases.	63	"Security specialists should attend sprint-0 and architecture workshops."
Clarify Security Roles & Tasks	Issue a clear RACI* for security ownership, decision-making, and sign-off.	58	"Assign who reviews code for vulnerabilities and who approves fixes."
Improve Cross-Team Communication	Increase structured interactions between PM, dev, ops, and security teams.	53	"Schedule joint stand-ups so dev and security can discuss threats in real time."
Adopt Standard Frameworks	Use recognized frameworks (e.g., NIST CSF, ISO 27001, OWASP SAMM) to guide practice.	46	"Following NIST keeps us aligned and avoids reinventing controls."

Key Insights:

The qualitative results indicated that training was the most valuable approach to improve the integration of cybersecurity practices, and identified the need for ongoing and role-specific training. The participants highlighted the need for cyber security professionals to play a role from the project's very inception, have clear roles and responsibilities, and for cross functional teams to be used effectively. The introduction of standard cybersecurity frameworks is also seen to be beneficial to improve the consistency, maturity of the organization, and matching with the best practices in the industry.

The findings align with the quantitative data and confirm that it is these organizational abilities—the ability to collaborate, train, and apply organized cybersecurity practices—that enable enhancements in project management in software engineering. The priority of strategies for improvement is demonstrated in Figure 4.

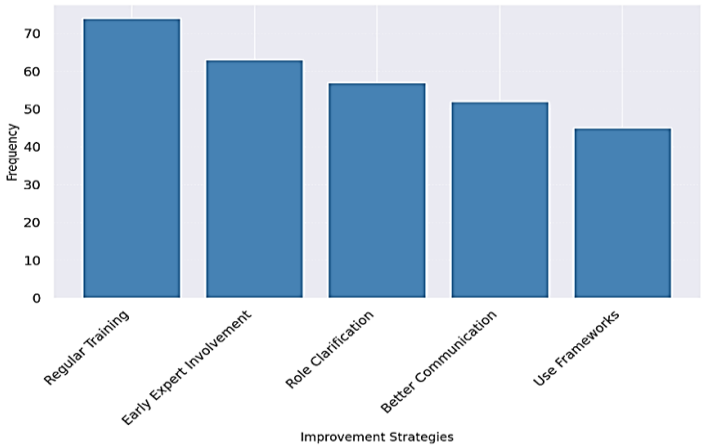

Figure 4: Improvement Strategies

The research examined the effect of cybersecurity practices on software engineering project management in the areas of time, budget, team work and risk management. Results confirm Dynamic Capability Theory positing that cybersecurity is more a matter of technology or compliance. Applying cybersecurity practices to software development processes is able to strengthen resilience and help efficiently manage resources and achieve project goals. The major outcomes of the research are discussed below in relation to the previous research findings concerning the matter. The results can be seen from the perspective of Dynamic Capabilities Theory, which highlights the organization's ability to sense threats, seize the moment by obtaining and utilizing needed resources, and adapt its systems and processes. As a result, the importance of preparedness in terms of risk management ($\beta = 0.491$, $p < 0.001$) shows that organizations which habitually assess the nature of cyber threats can detect those threats before they show themselves practically. In connection to that, the meaning of cybersecurity budgeting supports the idea of seizing capabilities because the allocated resources would allow the organization to react to different risks rather than just recognize them. Finally, the effect of early inclusion of security into SDLC ($\beta = 0.353$, $p < 0.001$ as for timeline) indicates the organization's ability for reconfiguring because security becomes part of the system, thus helping organizations to adapt to the new threats which arise in the process of change.

1. importance of risk management: Preparedness in the area of risk management has proven to be the most reliable indicator of the success of a project ($\beta = 0.491$, $p < 0.001$). Projects that had a plan for the assessment of risk and measures to reduce risk hardships were better prepared in terms of timely resolution of delays and budget overruns. The outcome we received corresponds with a research conducted by Humayun et al. [22] where a reliable SDLC framework has placed a strong emphasis on continuous monitoring of the effectiveness of risk management within projects relying totally on cooperation of the teams.
2. effects of timelines — fiction or reality: Almost all the respondents have believed that the presence of cybersecurity practices would make the projects take longer to complete (mean = 3.52/5). Nevertheless, the analysis of regression points at the importance of integrating preventative cybersecurity measures early on so as to avoid possible disruptions in the flow of projects ($\beta = 0.353$, $p < 0.001$). The present finding contradicts the widespread belief about the ability of security processes to hamper the cycle of development and proves the value of integrated agile/security project-management methods [9].

The following valuable solutions can be utilized by software engineering companies and project managers:

1. Early incorporation of cybersecurity: Including cybersecurity components in project planning and design facilitates prediction and decreases the chances of schedule failures.
2. Special budgets for cybersecurity: Setting aside some funds specifically for cybersecurity allows for more efficient use of resources and better resource planning.
3. Periodic training based on roles: Training employees on cybersecurity on a continuous basis increases their awareness and makes cybersecurity a part of project development teams.
4. Application of cybersecurity frameworks: The application of frameworks like NIST CSF, ISO/IEC 27001, and OWASP SAMM helps improve governance, defines security responsibilities, and allows more consistent application of cybersecurity in the software development process.

4. CONCLUSION

The purpose of this research was to quantitatively survey the impact of cybersecurity practices on software engineering project management. While providing additional evidence that cybersecurity contributes to better project performance, this study makes its primary contribution at the theoretical level by characterizing cybersecurity as an organizational capability that is dynamic in nature. Framing how security is implemented in

terms of sensing, seizing, and reconfiguring to deal with cyber-risk contributes Dynamic Capabilities Theory to a field (software project management) where it has been seldom used empirically. From a practitioner's standpoint, this means four things. Ensure cybersecurity is considered from early in the software development lifecycle (helping assure predictability, not hindering it), allocate budgets specifically for cybersecurity (helping you plan and manage risk based on actual resources), provide continued, role-based security training (it's an investment, not a one-time expenditure), and use frameworks like the NIST CSF, ISO/IEC 27001, and OWASP SAMM to help define security roles and maintain governance throughout development. Addressing these four areas can help shift cybersecurity from being viewed as a cost center or blocker to an enabler of predictable, successful projects.There are some limitations to this study. The results are limited to self-reported data from surveys of 128 practitioners and may not be generalizable. Since purposive sampling was used, there is potential for selection bias. Organizations that agreed to participate were those with previous experience with cyber security implementation. Future studies can explore the impact of cybersecurity efforts over longer durations including entire development lifecycles, differences in cybersecurity governance between Agile vs. traditional project environments, and utilization of AI to aid cybersecurity risk evaluation and decision-making for software engineering projects. In conclusion, this research shows that when cybersecurity is designed into software products from the start, projects have more predictable and secure outcomes that lead to success.

ACKNOWLEDGEMENTS
The authors thank the University of Mosul/ College of Computer Sciences and Mathematics for the facilities that enhanced the quality of this work.

REFERENCES

[1] M. T. Baldassarre, V. S. Barletta, D. Caivano, and M. Scalera, “Integrating security and privacy in software development,” *Software Quality Journal*, vol. 28, no. 3, pp. 987–1018, 2020, doi: 10.1007/s11219-020-09501-6.

[2] D. J. Ferreira, N. Mateus-Coelho, and H. S. Mamede, “Methodology for Predictive Cyber Security Risk Assessment (PCSRA),” *Procedia Computer Science*, vol. 219, pp. 1555–1563, 2023, doi: 10.1016/j.procs.2023.01.447.

[3] M. F. Harake, "Integrating Cybersecurity into Project Management: Best Practices, Emerging Trends, and Strategic Approaches," PM World Journal, vol. XIV, no. I, pp. 1–38, Jan. 2025.

[4] V. Tynchenko et al., "Adaptive Management of Multi-Scenario Projects in Cybersecurity: Models and Algorithms for Decision-Making," *Big Data and Cognitive Computing*, vol. 8, no. 11, art. no. 150, 2024, doi: 10.3390/bdcc8110150.

[5] M. S. Farooq, A. Hamid, A. Alvi, and U. Omer, “Blended Learning Models, Curricula, and Gamification in Project Management Education,” *IEEE Access*, vol. 10, pp. 60341–60361, 2022, doi: 10.1109/ACCESS.2022.3180355.

[6] Federal Bureau of Investigation and Cybersecurity and Infrastructure Security Agency, "#StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability," Joint Cybersecurity Advisory AA23-158A, Jun. 7, 2023.

[7] H. M. Yahya and D. B. Taha, “Detection Bad Code Smells By Using Deep Machine Learning Approaches,” in *2023 1st International Conference on Advanced Engineering and Technologies (ICONNIC)*, 2023, pp. 281–286, doi: 10.1109/ICONNIC59854.2023.10467672.

[8] M. A. Akbar, A. A. Khan, N. Islam, and S. Mahmood, “DevOps project management success factors: A decision-making framework,” *Software: Practice and Experience*, vol. 54, no. 2, pp. 257–280, 2024, doi: 10.1002/spe.3269.

[9] P. Amajuoyi, L. B. Benjamin, and K. B. Adeusi, “Optimizing agile project management methodologies in high-tech software development,” *GSC Advanced Research and Reviews*, vol. 19, no. 2, pp. 268–274, 2024, doi: 10.30574/gscarr.2024.19.2.0182.

[10] National Institute of Standards and Technology, “Advanced Encryption Standard (AES),” U.S. Department of Commerce, 2023.

[11] G. McGraw, “Software security,” *IEEE Security & Privacy*, vol. 2, no. 2, pp. 80–83, 2004.

[12] M. Parveen and M. A. Shaik, “Review on penetration testing techniques in cyber security,” in *2023 Second International Conference on Augmented Intelligence and Sustainable Systems (ICAISS)*, 2023, pp. 1265–1270, IEEE.

[13] M. Howard and S. Lipner, *The Security Development Lifecycle*. Redmond, WA, USA: Microsoft Press, 2006.

[14] H. Tyagi and S. Watanabe, *Information-Theoretic Cryptography*. Cambridge, U.K.: Cambridge University Press, 2023, doi: 10.1017/9781108670203.

[15] Project Management Institute, *A Guide to the Project Management Body of Knowledge (PMBOK® Guide) and The Standard for Project Management*, 7th ed. Newtown Square, PA, USA: Project Management Institute, 2021.

[16] M. Stadnyk and A. Palamar, "Project management features in the cybersecurity area," *Scientific Journal of the Ternopil National Technical University*, vol. 106, no. 2, pp. 54–62, 2022, doi: 10.33108/visnyk_tntu2022.02.054.

[17] H. van Zyl, "The ranking of dimensions for project-management efficiency in the public sector," *Journal of Economic and Financial Sciences*, vol. 1, no. 1, pp. 39–50, 2007, doi: 10.4102/jef.v1i1.378.

[18] C. Battistella, T. Bortolotti, S. Boscari, F. Nonino, and G. Palombi, "The impact of cultural dimensions on project management performance," *International Journal of Organizational Analysis*, vol. 32, no. 1, pp. 108–130, 2024, doi: 10.1108/IJOA-11-2022-3498.

[19] OWASP Foundation, *OWASP Secure Coding Practices – Quick Reference Guide*, ver. 2.1. OWASP Foundation, 2022.

[20] R. Potturi, "Integrating Cybersecurity into Project Management: A Comprehensive Approach Across SDLC Phases," *ISACA Journal*, vol. 4, Jul. 2024. [Online]. Available: https://www.isaca.org/resources/isaca-journal/issues/2024/volume-4.

[21] S. Kumar and G. Nagar, "Threat Modeling for Cyber Warfare Against Less Cyber-Dependent Adversaries," *European Conference on Cyber Warfare and Security*, vol. 23, no. 1, pp. 257–264, 2024, doi: 10.34190/eccws.23.1.2462.

[22] M. Humayun, N. Z. Jhanjhi, M. F. Almufareh, and M. I. Khalil, "Security threat and vulnerability assessment and measurement in secure software development," *Computers, Materials & Continua*, vol. 71, no. 3, pp. 5039–5059, 2022, doi: 10.32604/cmc.2022.019289.