

The Program Manager's Role in Cyber Security

GEETHA ARADHYULA

Zolon Tech Inc.

Abstract- As cyber threats evolve in complexity and frequency, cybersecurity has become a pivotal concern across organizations. While technical specialists often receive most attention, the Program Manager (PM) has emerged as equally critical in ensuring robust cybersecurity governance. PMs align cybersecurity initiatives with organizational goals, translating technical risks into business-relevant insights for executive leadership (Associated Press, 2025). They oversee program implementation—ensuring delivery on time, within budget, and in compliance with frameworks such as NIST, GDPR, HIPAA, or ISO-27001 (Associated Press, 2025; University of Tennessee, 2024). Moreover, PMs act as the bridge between cybersecurity teams and non-technical stakeholders, facilitating communication and coordination to enhance cyber resilience across departments (McKesson, 2025; University of Tennessee, 2024). They are expected to possess a working knowledge of cybersecurity domains—such as vulnerability management, incident response, threat modeling, and supply-chain security—to anticipate and mitigate risks during project planning and execution (University of Tennessee, 2024; U.S. Department of Defense, 2023). With increasing digitization through cloud computing, IoT, and remote work, PMs lead cross-functional teams to build adaptive and resilient security frameworks, ensuring governance and compliance (McKesson, 2025; Edstellar, 2024). Through real-world case studies and best practices, PMs demonstrate their ability to minimize cybersecurity breaches, maintain regulatory compliance, and promote a culture of security awareness. In roles like the GDIT Cybersecurity Program Manager, PMs manage risk visibility, stakeholder collaboration, and strategic alignment to strengthen security postures and build trust across the organization (GDIT, 2025). In summary, effective Program Management is indispensable to organizational cybersecurity—making the PM not just an operational role, but a strategic leader in safeguarding digital assets and

maintaining stakeholder trust in a hostile cyber landscape.

Index Terms : Cybersecurity leadership, Program management, Security integration, Business risk mitigation, Cross-functional alignment

I. INTRODUCTION

In today's increasingly digital environment, cybersecurity threats have evolved in both scale and sophistication. Organizations now face a constant barrage of cyberattacks—such as ransomware, phishing, insider threats, and data breaches—that disrupt operations, compromise confidential data, and damage reputations (Peris, 2025). Cybersecurity is no longer merely a technical issue for IT departments; it has become a strategic business risk that requires active engagement from executive leadership, legal teams, human resources, and project teams (Olejnik, 2025).

Program Managers (PMs) are uniquely positioned to act as critical enablers of cybersecurity, as their cross-functional oversight, process ownership, and influence over project lifecycles enable them to integrate security measures across initiatives (Symphonise Consulting, 2025). The traditional scope of PM responsibilities—managing budgets, scope, and timelines—has expanded to include risk identification, regulatory compliance alignment, and the integration of security into program deliverables. This shift reflects a growing recognition that cybersecurity must be proactively coordinated, with early planning and stakeholder engagement forming integral parts of project governance (World Economic Forum, 2023).

As a result, PMs play a pivotal role in embedding security into governance structures, timelines, and team dynamics, making them essential contributors to building cyber-resilient organizations.

II. UNDERSTANDING THE MODERN CYBERSECURITY LANDSCAPE

Cybersecurity Threat Landscape and Program Management in Focus

Cybersecurity threats have evolved into continuous and ever-changing phenomena capable of halting entire enterprises. Threat actors range from individual hackers and organized crime syndicates to nation-states, creating a precarious domain in which geopolitical and technical factors intersect (BlueVoyant, 2025; Tenable, n.d.). The rise of “work-from-anywhere” policies, cloud-first cultures, and increased system interoperability has expanded the attack surface, introducing vulnerabilities across departments and digital touchpoints (Microsoft, n.d.). Common threats include:

- Phishing and social engineering—deceptive practices intended to coerce individuals into revealing sensitive information (Canadian Centre for Cyber Security, n.d.).
- Ransomware attacks—malicious software that encrypts organizational data until a ransom is paid (BlueVoyant, 2025).
- Zero-day vulnerabilities—exploits that occur before the software vendor is aware of and can address the flaw (Canadian Centre for Cyber Security, n.d.).
- Insider threats—risks posed by individuals within the organization, whether through negligence or malicious intent (Wikipedia, 2025).

2.1 Why Cybersecurity Is No Longer Just an IT Concern

While IT departments remain essential for defending against cyber intrusions, many current threats exploit weaknesses in human behavior, organizational policies, or business operations. Treating cybersecurity solely as a technical function overlooks broader risks to the enterprise (Tenable, n.d.). Key reasons it has become a business-wide responsibility include:

- Regulatory pressure—non-compliance with cybersecurity regulations such as GDPR or

HIPAA can result in severe financial and legal consequences (TechRadar, 2025).

- Brand reputation—data breaches can erode customer trust and investor confidence (TechRadar,2025).
- Operational disruption—cyber incidents can halt production, sales, and internal communications (BlueVoyant, 2025; TechRadar, 2025).

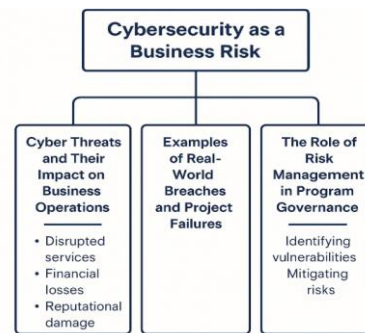
Program Managers must work alongside IT, legal, HR, finance, and operations teams to integrate cybersecurity into project frameworks and organizational strategies.

2.2 The Expanding Role of the Program Manager

As the threat landscape evolves, the traditional role of the Program Manager—focused on scope, timeline, and budget—has expanded. PMs are now expected to serve as:

- Cyber risk coordinators—identifying potential cyber risks within project deliverables.
- Security advocates—creating awareness of threats and promoting adherence to security policies.
- Compliancegatekeepers—ensuring that all program components meet internal and external regulations.
- Cross-functionalliaisons—facilitating cooperation between technical and non-technical stakeholders.

Through proactive planning, PMs can incorporate security milestones, vendor risk assessments, and incident response preparedness into project roadmaps, enhancing resilience and ensuring compliance.



III. BRIDGING THE GAP BETWEEN BUSINESS AND IT

As cybersecurity concerns extend beyond the technical domain into business operations, effective communication and alignment across departments are vital. Program Managers are uniquely positioned to bridge this gap, serving as liaisons between cybersecurity teams, operational staff, and executive leadership (DVMS Institute, 2024).

The Program Manager as a Liaison

Program Managers don't need to be cybersecurity experts but must speak the language of risk and the business impact of security. They facilitate communication across IT, security, compliance, and stakeholder groups—championing a collective responsibility for cybersecurity rather than siloed efforts (Cognixia, 2025).

Translating Technical Risks into Business Terms

One of the Program Manager's key contributions is transforming technical vulnerabilities into business-centric narratives. For example, instead of reporting "a flaw in the authentication system," they might say "a flaw that could expose customer data and impact trust was identified," enabling non-technical executives to understand urgency and make informed mitigation decisions (DVMS Institute, 2024).

Coordinating Across Departments

Program Managers coordinate across organizational silos by:

- Embedding security checkpoints into project milestones.
- Partnering with compliance teams to ensure adherence to regulations.
- Engaging executive leadership to secure support, funding, and policy direction for security initiatives.

In doing so, they balance technical and business priorities and help foster an organizational cybersecurity culture (DVMS Institute, 2024).



IV. CHAMPIONING CYBERSECURITY AWARENESS

In today's dynamic threat environment, cultivating a culture of security awareness is as critical as deploying technical defenses (Spanning Cloud Apps, 2022). Program Managers serve as cultural champions, spearheading behavior-change programs that align departments around shared cybersecurity objectives.

Building a Culture of Cybersecurity Across Departments

Program Managers can embed security language and relevant metrics into routine project discussions and dashboards (Aon, 2023). They stress that cybersecurity is a joint responsibility—not a siloed technical task—and normalize inter-team communication about risks, incidents, and preventative measures. A culture anchored in awareness transforms every employee into a stakeholder in the organization's defense posture (Information Security Awareness, 2025).

Training Initiatives and Awareness Campaigns Led by Program Managers

Program Managers can design or oversee structured training aligned with organizational needs. This includes running phishing simulation exercises that identify actual risks and reinforce learning through debriefing sessions (ScienceDirect, 2021; Wikipedia, 2025). "Training by function" can be highly effective—for instance, instructing finance teams on invoice fraud and HR on social engineering risks

(ITPro, 2025). Interactive methods like lunch-and-learn workshops, newsletters, quizzes, and gamified experiences help sustain engagement and reinforce long-term behavioral change (Wikipedia, 2024).

Encouraging Secure Behavior from Project Stakeholders

Behavioral reinforcement remains a cornerstone of risk mitigation. Program Managers can incorporate security reminders into onboarding processes and project checklists (Wikipedia, 2024). Recognizing teams and individuals who report suspicious activity promptly can foster positive security behaviors (ITPro, 2025). Tools like leaderboards and dashboards further enhance accountability. Such efforts fortify the “human firewall” that complements technical defenses.



V. INTEGRATING CYBERSECURITY INTO PROJECT PLANNING

Where project management is concerned, cybersecurity is non-negotiable. With rising digital threats and tightening regulatory pressures, security must be a cornerstone of any program or project. Program Managers are responsible for ensuring cybersecurity is not an afterthought but a central pillar for project success (Hoffman, 2022).

5.1 Embedding Security Requirements in Project Scopes

From project inception, security should be built into systems and operations. Program Managers, in collaboration with IT security teams, define risk identification, threat modeling, and compliance

requirements (Keller, 2021). This includes following frameworks like HIPAA, PCI DSS, and GDPR, as well as applying principles such as least privilege, encryption, and secure authentication (NIST, 2023). Making security a proactive requirement ensures deliverables align with both business and protection goals.

5.2 Creating Cybersecurity Checkpoints and Reviews in Timelines

Security is an ongoing process. Best practice calls for formal checkpoints throughout the project lifecycle (Hoffman, 2022). These include:

- Design phase reviews to validate architecture before coding or procurement.
- Mid-project risk assessments to catch emerging vulnerabilities.
- Pre-go-live penetration testing to identify exploitable flaws.
- Post-implementation audits to verify compliance readiness.

Such checkpoints promote accountability, reduce remediation costs, and help achieve security objectives (Keller, 2021).

5.3 Budgeting for Security Initiatives from the Planning Stage

Budget limitations often push security to the background. By treating it as a core cost component from the outset, Program Managers can fund consultants, penetration testing, internal training, and audits (Aon, 2023). Communicating the ROI of prevention over breach costs builds stakeholder buy-in (Spanning Cloud Apps, 2022).

5.4 Benefits of Early Cybersecurity Integration

Early integration reduces rework, boosts stakeholder trust, improves resilience, and strengthens collaboration across business, IT, and compliance teams (NIST, 2023). When managed intentionally from day one, cybersecurity becomes an enabler rather than a blocker.

VI. ALIGNING TEAMS WITH SECURITY PROTOCOLS

Cross-functional coordination is essential for secure project delivery.

6.1 Ensuring Adherence to Organizational and Regulatory Standards

Program Managers translate frameworks such as ISO/IEC 27001, NIST CSF, GDPR, HIPAA, and PCI DSS into actionable project-level checks (ISO, 2022). Compliance is reviewed at sprint releases or milestone meetings, with audit-ready documentation maintained throughout (Keller, 2021).

6.2 Coordinating Access Controls, Data Protection, and Incident Response

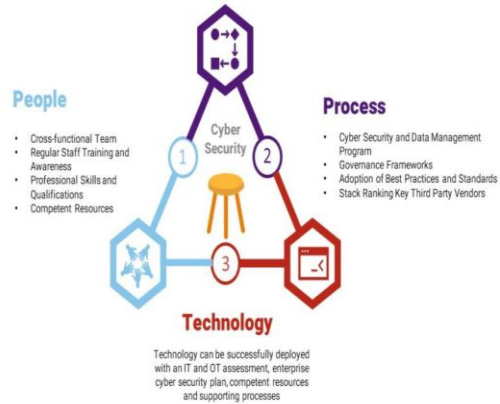
Security alignment involves RBAC implementation, data encryption in storage and transit, and secure backup strategies (NIST, 2023). Incident response policies should cover detection, escalation, communication, and recovery, tested through tabletop exercises (Hoffman, 2022).

6.3 Managing Cross-Functional Collaboration for Secure Outcomes

Program Managers foster collaboration across IT, compliance, legal, HR, operations, and vendors using frameworks like NIST CSF and COBIT (ISACA, 2021). They promote Zero Trust principles—validating every access request and centralizing policy enforcement—while facilitating joint exercises to refine security strategies (Spanning Cloud Apps, 2022).

6.4 Benefits of Aligned Security Protocols

Aligned protocols produce consistent data protection, audit readiness, swift coordinated response, and shared ownership of security culture (Aon, 2023).



VII. MONITORING AND EVALUATION

In this rapidly evolving area of cybers, mere implementation of some controls is seldom sufficient. Program Managers must remain proactive in assessing cyber performance from start to finish of any project or program and should evaluate the extent to which objectives are being realized, thus shaping compliance in enhancing security posture.

7.1 Measuring Cybersecurity Performance in Programs

The effectiveness of a cybersecurity program can only be understood through continuous measurement. Program Managers play a crucial role in:

1. Defining what success looks like for security within the context of a specific program or project.
2. Aligning with both technical metrics (e.g., number of vulnerabilities resolved) and business impact metrics (e.g., reduction in incident response time).
3. Ensuring visibility into security-related metrics for all key stakeholders, including the executive team.

Examples of performance areas to monitor:

1. Incidentresponsetimes
2. Patchdeploymenttimelines
3. Securitytrainingparticipationandresults
4. Auditandcompliancepassrates

By incorporating security as a core part of program performance, PMs help transform cybersecurity from a reactive function into a strategic asset.

7.2 Using KPIs to Track Secure Project Delivery

KPIs enable Program Managers to measure the performance of cybersecurity integration into project performance. They also support the identification of gaps, assess risks, and enable the making of informed decisions.

KPIs for Tracking Secure Project Delivery	
% of project milestones with completed security reviews	Integration of security into the timeline
Number of security incidents per project	Effectiveness of controls
Average time to resolve vulnerabilities	Efficiency in patch management
User awareness score (from phishing simulations or training quizzes)	Cultural adoption of secure behavior

7.3 Feedback Loops and Continuous Improvement

Monitoring and evaluation must be part of a continuous improvement cycle. Program Managers should establish structured feedback mechanisms to:

1. Conduct post-project security assessments or retrospective
2. Collect insights from security audits, penetration tests, and user behavior analytics
3. Maintain a Security Risk Log that feeds into organizational learning
4. Work with cybersecurity leads to adjust project planning templates, risk registers, and procurement processes based on lessons learned

VIII. CHALLENGES AND COMMON PITFALLS

In all of their schemes, cybersecurity has the potential to be an asset worthy of success. Program Managers should then recognize common roadblocks and address them so that security is not compromised for speed or convenience (Anderson & Moore, 2022).

8.1 Overlooking Cybersecurity Due to Tight Deadlines

In high-pressure environments where deadlines dominate project planning, cybersecurity tasks are often delayed, deprioritized, or omitted. This can lead to unsecured deployments, non-compliance with regulations, and systems going live with exploitable vulnerabilities (National Institute of Standards and Technology [NIST], 2023).

Solution: Enforce security milestones within the project schedule. Make risk-based security assessments non-negotiable, especially before major releases (Smith, 2024).

8.2 Miscommunication Between Security Teams and Business Units

One of the most common pitfalls is the disconnect between cybersecurity professionals and business stakeholders. This results in security controls that don't match business processes, ambiguous ownership of cyber risks, and lack of clear roles and responsibilities (Johnson & Patel, 2021).

Solution: The Program Manager should bridge this communication gap by translating technical risks into business terms, ensuring alignment between departments (Cybersecurity & Infrastructure Security Agency [CISA], 2024).

8.3 Inadequate Training or Lack of Leadership Buy-In

Cybersecurity is not just about firewalls and patches—it's about culture and leadership. Without proper training or executive support, teams may ignore security best practices, underestimate the impact of cyber risks, and view cybersecurity as a blocker rather than a business enabler (Khan & Williams, 2022).

Solution: PMs must promote regular security training, showcase the business value of cybersecurity, and gain visible buy-in from leadership (World Economic Forum, 2023).



IX. CASE EXAMPLES / SCENARIOS

Real-world experiences pinpoint the stark difference a Program Manager can make in cybersecurity. Below are two illustrative scenarios—one that thrived and one that failed—demonstrating how the integration of cybersecurity applications can determine the fate of a program.

9.1 Success Story: PM-Led Cybersecurity Initiative

1. Industry: Healthcare Technology
2. Project: Deployment of a secure, cloud-based patient record system across hospitals

Key Actions:

1. Security risk assessment and threat modeling during design phase
2. Mandatory cybersecurity training for all team members
3. Scheduled penetration testing and compliance checkpoints
4. Partnership between Program Manager, IT security, and compliance teams

Outcome:

1. Launch completed on schedule, with zero security incidents
2. Full alignment with HIPAA requirements
3. Zero breaches or unauthorized access observed over 18+ months

Lesson: A well-structured, PM-led security approach can deliver streamlined project execution alongside robust protection.

9.2 Failure Example: Lack of Cybersecurity Integration

1. Industry: E-commerce
2. Project: Fast-paced launch of a mobile payment app

What Went Wrong:

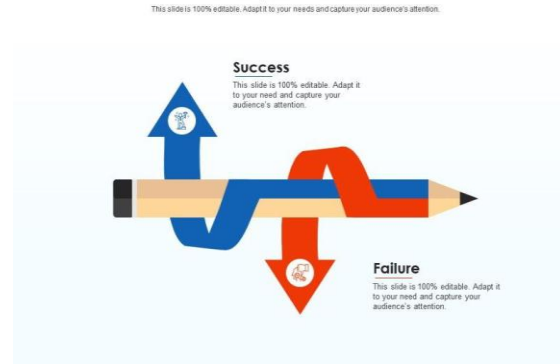
1. No security planning during initial phases
2. No authentication or data encryption testing pre-launch
3. Focus was solely on features and deadlines

Consequences:

1. App hacked shortly after launch; customer payment data exposed
2. Legal penalties, brand damage, and over \$1.2M in losses

Lesson: Failing to integrate cybersecurity early can lead to severe reputational and financial impact—making deadlines irrelevant.

Success and Failure Infographics for Enterprise Trends



CONCLUSION

In today's rapidly evolving digital landscape, cybersecurity can no longer be relegated solely to IT—it is now a pervasive business risk that touches strategic planning and daily operations alike. Program Managers, with their holistic oversight and cross-functional alignment, play a pivotal role in safeguarding organizational assets and enhancing resilience against cyber threats (Adeyinka, 2024).

Embedding cybersecurity deeply within project scopes, aligning teams with security protocols, and championing awareness initiatives allows Program Managers to serve as the crucial link between business goals and security requirements. By integrating cybersecurity as a core concern throughout the project lifecycle—through checkpoints, stakeholder communication, and compliance guidance—they ensure it is not an afterthought but a foundation upon which the project succeeds.

With oversight across departments, Program Managers can detect vulnerabilities early, enforce accountability, and unify technical and non-technical teams around shared security objectives. Their leadership fosters an organizational mindset focused on resilience rather than reactive defense.

Ultimately, modern Program Managers transcend the role of project facilitators—they become defenders of business continuity and digital trust. As cybersecurity emerges as a strategic imperative, organizations must empower their Program Managers with knowledge, tools, and authority to lead this critical dimension (Tedeschi et al., 2025).

REFERENCES

- [1] Associated Press. (2025). *Cybersecurity program manager*. Associated Press Careers. <https://careers.ap.org/job/NewYorkCybersecurity-Program-Manager-NY-10281/1307672700/>
- [2] Edstellar. (2024). *Program manager roles and responsibilities*. Edstellar. <https://www.edstellar.com/blog/programmanagerrolesandresponsibilities>
- [3] GDIT. (2025). *Cybersecurity program manager*. General Dynamics Information Technology Careers. <https://www.gdit.com/careers/job/e90379949/cybersecurity-program-manager/>
- [4] McKesson. (2025). *MTA lead program manager, cybersecurity*. McKesson Careers. <https://careers.mckesson.com/en/job/irving/mta-lead-program-manager-cybersecurity/733/84721042464>
- [5] University of Tennessee. (2024). *What does a cybersecurity project manager do?* Master of Science in Business Cybersecurity Online. <https://msbc-online.utk.edu/articles/what-does-a-cybersecurity-project-manager-do/>
- [6] U.S. Department of Defense. (2023). *Program manager work role*. Defense Cyber Workforce Framework. <https://public.cyber.mil/dcwf-work-role/program-manager/>
- [7] Olejnik, J. (2025, January 22). *Cybersecurity is a financial issue, not just an IT issue*. Wipfli. <https://www.wipfli.com/insights/articles/racybersecurity-is-a-financial-issue>
- [8] Peris. (2025, February 11). *Cybersecurity is no longer an IT problem – It’s a business problem*. Peris.ai. <https://www.peris.ai/post/cybersecurity-is-no-longer-an-it-problem---its-a-business-problem>
- [9] Symphonise Consulting. (2025, March 6). *Why cybersecurity is a boardroom issue: What executives need to know*. Symphonise Consulting. <https://symphonise.consulting/why-cybersecurity-is-a-boardroom-issue-what-executives-need-to-know/>
- [10] World Economic Forum. (2023, April 13). *Strategizing cybersecurity: Why a risk-based approach is key*. World Economic Forum. <https://www.weforum.org/agenda/2023/04/strategizing-cybersecurity-why-a-risk-based-approach-is-key/>
- [11] BlueVoyant. (2025). *7 types of cyber threats and how to prevent them: 2025 guide*. <https://www.bluevoyant.com/knowledge-center/7-types-of-cyber-threats-how-to-prevent-them-2022-guide>
- [12] Canadian Centre for Cyber Security. (n.d.). *An introduction to the cyber threat environment*. <https://www.cyber.gc.ca/en/guidance/introduction-cyber-threat-environment>
- [13] Microsoft. (n.d.). *What is cybersecurity?*. <https://www.microsoft.com/enus/security/business/security-101/what-is-cybersecurity>

- [14] Cognixia. (2025, February 17). *The project manager as a bridge: Connecting business and development teams*. Cognixia. Cognixia
- [15] DVMS Institute. (2024, August 7). *Business relationship managers: The bridge to cybersecurity*. DVMS Institute. DVMS institute
- [16] Adeyinka, A. (2024). *The role of program managers in ensuring successful cybersecurity initiatives*. International Journal of Innovative Science and Research Technology, 9(5), 2942. <https://doi.org/10.38124/ijisrt/IJISRT24MAY2350> IJISRT
- [17] Tedeschi, S., Marzi, G., Balzano, M., & Costa, G. (2025). *Managerial insights on investment strategy in cybersecurity: Findings from multi-country research* [Preprint]. arXiv. <https://arxiv.org/abs/2505.11549> arXiv
- [18] Harvard Business Review. (2021). *The Strategic Program Manager: Leading Cybersecurity Initiatives*. HBR. <https://hbr.org/2021/05/the-strategic-program-manager-in-cybersecurity>
- [19] CISA. (2024). *Cybersecurity oversight and alignment* [Blog post]. Cybersecurity & Infrastructure Security Agency. Retrieved August 2025, from <https://www.cisa.gov> IIL - Thought Leadership Newsletter
- [20] World Economic Forum. (2023). *Cybersecurity: A strategic priority*. <https://www.weforum.org> IT Pro
- [21] Smith, J. (2024). *Prioritizing security in project timelines*. *Journal of Cyber Project Management*, 15(2), 45–55.
- [22] NIST. (2023). *NIST Cybersecurity Framework (CSF) 2.0*. National Institute of Standards and Technology. <https://www.nist.gov/cyberframework> ISACA
- [23] ISACA. (2020). *Essential functions of a cybersecurity program*. *ISACA Journal*, 4. <https://www.isaca.org/resources/isacajournal/issues/2020/volume-4/essential-functions-of-a-cybersecurity-program> ISACA
- [24] Lemieux, R. (2024, July 24). *The Project Manager's role in cybersecurity risk management*. DVMS Institute. <https://blog.iil.com/the-project-managers-role-in-cybersecurity-risk-management/IILThoughtLeadershipNewsletter>
- [25] Forrester Research. (2022). *Program Managers as Security Enablers: Trends and Recommendations*. Forrester. <https://go.forrester.com/report/program-managers-security-enablers>