PROJECT MANAGEMENT GLOBAL
The Place for People in Projects

Securing the Future of Banking: Project Leadership's Critical Role in Addressing AI Implementation Challenges

April 29, 2025

The rapid spread of Artificial Intelligence (AI) across industries has been accompanied by a clear sense of excitement and urgency. The mantra repeated has been to "innovate or die," leading many organizations to embrace AI with remarkable speed. And with equal levels of hope and reckless abandonment of usual rigorous safeguards, in even the most protected fields such as finance, banking and legal where regulatory and fiduciary requirements are most stringent.

It is an issue that has not been overlooked by those at the helm of the project professional Bodies. A soon to be released report by the Project Management Institute (PMI) has promised to provide much needed guardrails for the implementation of AI Projects, across all industry realms.

However, a recent open letter from financial behemoth JPMorgan Chase to its third-party suppliers has injected a further dose of urgency into this fervent need for structured guidelines. Sounding a clear and urgent alarm about the precarious state of AI security particularly within the gated world of banking and finance.

JPMorgan's internal assessments paint a concerning picture, one that suggests many companies have prioritized deployment speed over fundamental security considerations.

The stark statistics revealed in their letter that a staggering **78% of enterprise AI deployments lack proper security protocols**, that most companies **cannot explain how their AI makes decisions**, and

that **security vulnerabilities have increased threefold since mass AI adoption**.

These matters underscore a systemic issue that demands immediate attention.

As project professionals, often on the frontline of delivering new AI technology, many are now question what can project leaders do to stem the flow of project failure in this area and can implementing basic but essential project disciplines improve the poor results that are being reported? Or whether a new and revolutionary way of instigating AI implementation is the best way forward.

As **JP Morgan's CTO, Pat Opet**, astutely observed, many organizations are deploying systems they fundamentally do not understand. This lack of comprehension, coupled with the breakneck pace of implementation, has created a fertile ground for significant risks, particularly within the highly regulated and financially sensitive financial sector, where trillions of dollars are at stake.

The consequences of this "speed over security" approach are multifaceted and potentially devastating. The lack of robust security protocols exposes organizations to increased risks of financial losses stemming from system vulnerabilities and cyberattacks. The inability to understand AI decision-making processes raises serious concerns about fraud detection and prevention, as malicious actors could potentially manipulate these opaque systems. Furthermore, the rush to deploy without proper planning and oversight inevitably leads to wasted resources on systems that are either ineffective, insecure, or ultimately unusable.

So, how can organizations navigate this increasingly risky landscape and mitigate their exposure? JPMorgan's recommendations offer a clear path forward. Emphasizing the critical role of improved project management, robust risk management, and effective governance in AI deployments:

1. Implement AI Governance Frameworks Before Deployment: This proactive approach necessitates establishing clear guidelines, responsibilities, and oversight mechanisms for all AI initiatives. A well-defined governance framework ensures that security and ethical considerations are baked into the project lifecycle from the outset, rather than being treated as afterthoughts. This includes defining acceptable use policies, data handling protocols, and accountability structures.

2. Conduct Regular Red Team Exercises Against AI Systems: Just as traditional cybersecurity benefits from penetration testing, AI systems require rigorous adversarial testing. "Red teaming" involves simulating attacks and attempting to exploit vulnerabilities in AI models and infrastructure. Regular exercises can identify weaknesses before they are exploited by malicious actors, allowing for timely remediation and strengthening of defenses.

3. Establish Clear Model Documentation Standards: The opacity surrounding AI decision-making is a major concern. Implementing clear and comprehensive documentation standards for AI models is crucial. This documentation should detail the model's architecture, training data, decision-making processes, limitations, and potential biases. Transparency not only aids in security assessments but also fosters trust and accountability.

4. Create Dedicated AI Security Response Teams: As AI systems become more complex and

integrated into core operations, organizations need specialized teams equipped to handle security incidents specific to AI. These teams should possess expertise in AI vulnerabilities, anomaly detection, and incident response strategies tailored to AI environments.

JPMorgan's own significant investment of $2 billion in AI security measures, coupled with a deliberate slowing of certain deployments, underscores the seriousness with which they view this issue. Their actions serve as a powerful example for other organizations to follow.

The hard truth, as JP Morgan aptly points out, is that the "AI security debt" is accumulating rapidly. Companies that fail to prioritize security now risk facing a severe reckoning in the future. The organizations that proactively address these vulnerabilities, implement robust governance, and prioritize security throughout the AI lifecycle will not only safeguard themselves from significant losses but will also emerge as leaders in this transformative technological era.

Better project leadership may play a pivotal role in improving the situation surrounding the risky deployment of AI. Effective project leadership, including planning and implementing a full project life-cycle approach can directly address the issues highlighted by JP Morgan by fostering a culture of responsibility, foresight, and meticulous execution, during and post project implementation. Here's how:

1. Setting a Security-First Vision and Culture:

- **Prioritization from the Top:** Strong project leaders can champion security as a core project objective, not just a secondary consideration. They can articulate a clear vision where secure and well-understood AI deployments are paramount, influencing the entire team's mindset.
- **Empowering Security Advocates, AI SMEs are Key throughout:** Leaders can identify and empower team members with security expertise, ensuring their voices are heard and their recommendations are integrated into the project plan. This creates a culture where security is everyone's responsibility, but specific expertise is valued and acted upon.

2. Defining Clear Objectives and Scope with Security in Mind:

- **Avoiding "Innovation at All Costs"**: Effective leaders can push back against purely speed-driven mandates, advocating for a more balanced approach that integrates security and understanding from the outset. They can define project success not just by the speed of deployment but also by the robustness and security of the implemented AI.
- **Breaking Down Complex Deployments:** Instead of rushing into large-scale, opaque AI deployments, strong leaders can advocate for a phased approach with clear milestones and security checkpoints at each stage. This allows for better understanding, testing, and securing of individual components before integration.

3. Ensuring Competent and Cross-Functional Teams:

- **Bridging the Gap Between AI Development and Security:** Project leaders can foster collaboration between AI developers, security experts, and domain specialists. This ensures that security considerations are integrated into the design and development process, and that the AI's functionality is well-understood by those responsible for its security.
- **Investing in Training and Expertise:** Leaders recognize the need for teams to possess the necessary skills to deploy and secure AI effectively. They can advocate for and facilitate training programs that equip team members with knowledge of AI security best practices, risk assessment methodologies, and governance frameworks.

4. Implementing Rigorous Planning and Risk Management:

- **Integrating Security into Project Plans:** Better project leadership ensures that security activities, such as threat modeling, vulnerability assessments, and penetration testing, are explicitly included in the project timeline and resource allocation.
- **Proactive Risk Identification and Mitigation:** Effective leaders foster a culture of proactive risk identification. They encourage teams to anticipate potential security vulnerabilities and develop mitigation strategies early in the project lifecycle, rather than reacting to issues after deployment.
- **Establishing Clear Communication Channels:** Leaders ensure open and transparent communication about potential security risks and mitigation efforts across all project stakeholders, including executive management and third-party suppliers.

5. Driving Adherence to Governance and Documentation:

- **Enforcing Governance Frameworks:** Strong project leaders take ownership of implementing and enforcing established AI governance frameworks. They ensure that the defined policies and procedures are followed throughout the project lifecycle and are built into future operations.
- **Championing Model Documentation:** Leaders emphasize the importance of clear and comprehensive model documentation and allocate the necessary resources for its creation, testing and maintenance. They understand that transparency is crucial for security, auditability, and ongoing management.

6. Facilitating Continuous Monitoring and Improvement:

- **Establishing Post-Deployment Security Measures:** Effective project leadership extends beyond the initial deployment. Ensure that robust monitoring and incident response mechanisms are in place to detect and address security threats in the operational phase.

- **Promoting a Culture of Learning and Adaptation:** Once in operation smart leaders will foster a mindset of continuous improvement, encouraging teams to learn from security incidents and adapt their processes and security measures accordingly. They recognize that the field of AI security is constantly evolving and requires ongoing vigilance and development.

Project leadership provides the necessary critical structure, oversight, and cultural foundation for a more secure and responsible deployment of AI. By prioritizing security from the outset, fostering collaboration, implementing rigorous planning, and enforcing governance, effective project management from the outset can significantly mitigate the risks highlighted by those on the front-line of banking security and pave the way for more trustworthy and sustainable AI adoption.

Find out more about project management in leading effective AI Adoption and Implementation, Change Management, Governance and Ethics in the banking and finance sector in the recommended reading texts below. And access thousands job opportunities in this and other sectors handpicked for PM Recruiter.

Note: This bibliography provides a starting point. For more specific reports and the latest research, consult the publications of major consulting firms, industry associations, academic databases, and government/regulatory bodies

AI Adoption and Implementation:

- **Brynjolfsson, E., & McAfee, A. (2017). *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies*.** W. W. Norton & Company. (Provides a broad context for the economic and societal impact of AI.)
- **Davenport, T. H., & Ronanki, R. (2018). Artificial Intelligence for the Real World.** *Harvard Business Review*, *96*(1), 108-116. (Offers practical insights into implementing AI in organizations.)
- **Manyika, J., Lund, S., Chui, M., Bughin, J., Woetzel, J., Batra, P., Ko, R., & Sanghvi, S. (2017).** *What the future of work will mean for jobs, skills, and wages*.McKinsey & Company. (Discusses the workforce implications of AI and the need for adaptation.)

Change Management:

- **Kotter, J. P. (2012). *Leading Change*.** Harvard Business Review Press. (A foundational text on the process of organizational change.)
- **Lewin, K. (1947). Frontiers in group dynamics: Concept, method and reality in social science; Social equilibria and social change.** *Human Relations*, *1*(1), 5-41. (Classic model of change management: Unfreeze, Change, Refreeze.)
- **Prosci. (Ongoing). *ADKAR Model*. (A goal-oriented change management model focusing on individual transitions.)**

AI Governance and Ethics:

- **Floridi, L., Cowls, B., Beltramini, M., Saunders, D., & Vayena, E. (2018). An ethical framework for a good AI society: opportunities, risks, principles, and recommendations.** *AI and Society*, *33*(4), 689-707. (Discusses the ethical considerations crucial for responsible AI deployment.)
- **Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate.** *Big Data & Society*, *3*(2), 2053951716679679.(Explores the ethical challenges posed by algorithmic decision-making.)
- **World Economic Forum. (Various Reports). *Focus on AI Governance and Ethics*.** (Search the WEF website for their publications on these topics.)

AI Security and Risk Management:

- **Brundage, M., Avin, S., Clark, J., Toner, M., Eckersley, P., Garfinkel, B., … & Zephyrin, D. (2018). *The malicious use of artificial intelligence: Forecasting, prevention, and mitigation*.** Future of Humanity Institute, University of Oxford. (Examines the potential security risks associated with AI.)
- **European Union Agency for Cybersecurity (ENISA). (Various Reports). *Focus on AI Security*.** (Check ENISA's website for reports and guidelines on securing AI systems.)
- **National Institute of Standards and Technology (NIST). (Ongoing). *AI Risk Management Framework*.** (A developing framework for managing risks associated with AI systems.)

Organizational Learning and Adaptation:

- **Senge, P. M. (2006). *The Fifth Discipline: The Art & Practice of the Learning Organization*.** Doubleday. (Provides insights into how organizations can learn and adapt to new technologies and challenges.)