Successfully Managing Cybersecurity Projects in the Age of AI[1]

Yogi Schulz

Managing cybersecurity projects in the age of AI has become more demanding. The stakes are higher. The cost to recover from a successful cyberattack is typically millions of dollars. The damage to reputation is significant but difficult to estimate.

In the age of large language models (LLMs) and generative AI, organizations must confront the security implications associated with these powerful technologies. Widespread attacker adoption of these technologies requires heightened responses to:

- Raise cybersecurity defenses.
- Maintain data privacy.
- Prevent data breaches and ransomware attacks.
- Reduce risks posed by shadow AI.

On a more positive note, adding LLMs and AI features to cybersecurity defenses can strengthen an organization's defenses against cybercriminals and keep its data safe.

Here's a list of topics cybersecurity project managers should address with their teams in their project management plan to ensure a successful cybersecurity project.

Project management best practices apply

Cybersecurity projects, with or without an LLM and AI, are not different from other IT projects. Sometimes, project teams convince themselves that cybersecurity projects are so profoundly technical that specialized individuals should be let loose to deliver them and that project management best practices don't apply.

Don't fall into this trap. Some cybersecurity deliverables are deeply technical. However, that's a reason to emphasize project management best practices, not abandon them.

Data scientists require management

Data scientists will be valued members of the cybersecurity project team. However, as their name states, these individuals are scientists, not IT professionals. Their culture, education, work

[1] How to cite this article: Schulz, Y. (2023). Successfully Managing Cybersecurity Projects in the Age of AI, *PM World Journal*, Vol. XII, Issue XII, December.

© 2023 Yogi Schulz

practices, organization expectations, attitudes, and reward systems differ from those of IT professionals. These differences can lead to conflicts and performance frustrations.

Project managers can mitigate these risks by coaching data scientists to:

- Focus on the cybersecurity deliverables and not be distracted by the many exciting insights they discover in the data.
- Restrict their work to the project scope and not explore the many enticing ideas that emerge during design discussions.
- Build robust software and avoid too many exploratory prototypes.
- Raise cybersecurity defenses and abandon the urge to write an academic paper about their project learnings.

Cybersecurity project risks

Project managers face the usual project risks plus a few new ones when managing cybersecurity projects. The risks include:

Project scope risks

To dramatically reduce cybersecurity risks, anxious stakeholders often push the cybersecurity project team to deliver an ambitious scope that exceeds the organization's skills and budget. The project team can reduce anxieties and facilitate a more factual discussion to refine the scope by:

- Achieving a consensus that the project goal is to raise the organization's cybersecurity defences because attackers are using AI and ML technology to mount more sophisticated attacks.
- Evaluating the organization's cybersecurity defences using one of several mature cybersecurity frameworks. The findings will be a list of gaps the team can prioritize for attention and use to build a scope consensus with stakeholders.
- Conducting a cybersecurity risk assessment. The team can use the prioritized risk list to build a functionality release plan that mitigates the higher impact risks and can be completed within the available project budget.
- Achieving a consensus that the project will use LLMs to strengthen the organization's cybersecurity defenses.

Project team skills and experience risks

Cybersecurity and AI/ML skills and experience are in demand as most organizations seek to raise their defences and reduce risks. Every recruiting website is overflowing with job postings. This situation will make it difficult to staff the project team with the desired skills and experience.

Staffing risks can be addressed by:

- Increasing compensation of project team members.
- Hiring understudies for some project team members.

- Planning for team turnover as some members are headhunted.
- Conducting a formal on-site training program.
- Enrolling project team members in various certification programs.

LLM vendor risks

Most organizations will license a vendor LLM and supporting software to raise their cybersecurity defenses rather than build their own LLM and supporting software.

Project teams will encounter vendor risks because many of these LLM vendors will be new and immature organizations with little track record. That creates difficult-to-mitigate risks.

Project managers will carefully reduce expectations with their project sponsor and stakeholders because difficulties will arise.

LLM and related software functionality risks

The project team can thoroughly evaluate the functionality of shortlisted LLMs and related software to reduce the risk of contracting for an inadequate or inappropriate LLM. Evaluation criteria to compare LLMs can include:

- References from other customers.
- Reviews on various websites.
- Available vendor support.
- Helpfulness of the customer community.
- Accuracy of the results generated.
- Speed or inference time to display results.
- Accuracy of grammar in results.
- Readability of results.
- Context length or limitations on prompt and results length.
- Quality and diversity of the training data.
- Model size – smaller tends to be faster, while larger is more precise.
- Indicators of bias in results.
- Bias detection and mitigation features.
- Explainability and availability of sources for the LLM's inferences.
- Guardrails for safety and responsibility.
- Degree of context understanding.
- Frequency of updates with recent information.
- Operating cost.
- Level of detailed and structured prompt engineering required to produce results.

Software stability risks

The AI- and ML-enhanced cybersecurity software vendors offer is brand new and has not been tested rigorously. The paint is likely still drying. Vendors are working overtime to add functionality

to their products as LLMs advance rapidly. To mitigate the risks of basing a project on unstable software, the project team should:

- Budget to test software thoroughly.
- Expect to install multiple releases of software during the course of the project.
- Monitor the vendor's software release notes regularly.
- Ensure that the team can roll back software to a previous version.
- Only promote software from test to production when the IT cybersecurity team is satisfied that it works reliably.

Software customization risks

Don't customize cybersecurity software packages. It's expensive and problem-prone. The biggest cost is re-applying the customizations for each new software version the vendor provides. This risk can be addressed by:

- Ensuring that the project team develops a comprehensive list of selection criteria to evaluate software packages. This list mitigates the risk of choosing software that won't fit the requirements.
- Including a statement in the project charter that the organization will adopt the cybersecurity management processes implicit in selected software packages.
- Including a statement in the project charter that the project team will not customize cybersecurity software packages.
- Participating in software vendors' customer advisory groups to propose new functionality the organization needs.

Do not confuse configuring software with customizing software. Configuring software is about setting values for variables the software package offers to tailor its operation. Customizing software is about writing and integrating new source code into the software package.

Management expectations risks

Senior management expectations for project costs, functionality and elapsed time often exceed available budget and organization capacity. This risk applies to cybersecurity projects because of management's lack of familiarity with such projects. Project managers can narrow the gap between expectations and reality by:

- Educating management on cybersecurity risks using summary case studies and not exaggerating.
- Having the team create a functionality release plan that illustrates how each release contributes to raising cybersecurity defenses.
- Reminding management that cybersecurity risk has already been partially addressed through previous work.

Project managers and their teams can deliver successful cybersecurity projects by proactively adhering to project management best practices and mitigating project risks.

About the Authors

Yogi Schulz

Calgary, Alberta, Canada

Yogi Schulz has over 40 years of Information Technology experience in various industries. Yogi works extensively in the petroleum industry to select and implement financial, production revenue accounting, land & contracts and geotechnical systems. He manages projects that arise from changes in business requirements, from the need to leverage technology opportunities and from mergers. His specialties include IT strategy, web strategy and systems project management.

Mr. Schulz regularly speaks to industry groups and writes a regular column for IT World Canada and for Engineering.com. He has written for Microsoft.com and the Calgary Herald. His writing focuses on project management and IT developments of interest to management. Mr. Schulz served as a member of the Board of Directors of the PPDM Association for twenty years until 2015. Learn more at https://www.corvelle.com/. He can be contacted at yogischulz@corvelle.com

His new book, co-authored by Jocelyn Schulz Lapointe, is "A Project Sponsor's Warp-Speed Guide: Improving Project Performance."