Security and Quality Issues in IT Projects

H. El Desouki and H. Armstrong

School of IS, Curtin University, Western Australia
e-mail: hassan.eldesouki@curtin.edu.au; helen.armstrong@curtin.edu.au

Abstract

The need for the inclusion of security and quality requirements early in the life of IT projects has been recognised for more than three decades. But have we learned from past experience? This paper presents four recent case studies of IT projects that have gone wrong for a variety of security and quality reasons. The problem is not a simple one to solve, however, valuable lessons can be learned from past experience. This paper relates to a project that is still a work-in-progress.

Keywords

Information security, quality assurance, IT project management.

1. Introduction and Background

Organizations and governments are more dependent than ever on reliable information systems. Yet organizations globally face an increased level of security threats that could undermine the operations of these systems. The problems associated with the lack of consideration of security and privacy issues in IT projects have been published for more than 30 years. For example early in the 1990's Borenstein (1991) claimed "the most likely way for the world to be destroyed, most experts agree, is by accident. That's where we come in; we're computer professionals. We cause accidents." Denning (1990:177) also highlighted the lack of security problems in IT stating "users, managers, and vendors routine fail to use sound security practices". Even at this early stage of IT applications in business Denning (1990:543) claimed we need to provide "adequate security, reliability, availability, performance and human safety" in our systems and networks. The lack of security and quality considerations in IT system developments was the focus of much research in the 1980's and 1990's. Neumann (1995:232) observed many "security-vulnerability exploitations result directly because of poor system and software engineering". Unfortunately, it appears the problems associated with lack of security in IT projects still exist.

The National Institute of Standards and Technology (Technology, 2006) highlighted that it is much more practical to implement security and quality from the beginning than later in the project lifecycle. "Experience in testing software and systems has shown that testing to high degrees of security and reliability is from a practical perspective not possible. Thus, one needs to build security, reliability, and other aspects into the system design itself and perform a security fault analysis on the implementation of the design". The most serious computer related accident to date in which people were killed is Therac-25 (Leveson & Turner, 1993). In 2010 the Toyota Motor Company issued a recall of its Prius hybrid vehicles, due to a software glitch that affected the braking system control (Valdes-Dapena & Lah, 2010). Organisations and individuals are relying on IT to achieve their goals. While many organisations do not place security and quality as high priorities in IT projects, quality problems, software defects and insecurity issues can actually kill and affect lives.

The primary focus of this paper is to present evidence that the problems of lack of security and quality factors identified three decades ago are still present in IT projects. This paper discusses several case studies of actual projects where specialists have been employed in the latter stages to alleviate the dilemmas associated with security and quality problems. These situations highlight the need for a new approach to the problem.

2. Research Methodology

The discussion within this paper forms a small part of a much larger project that aims to develop a methodology for late intervention in IT development projects where security and quality are key requirements. Data was collected from 30 IT Project Managers leading large, complex IT development projects, relating to problems the projects faced relating to the meeting of security and quality requirements within set time and budget ceilings. Four of the projects forming part of the original survey data were chosen for detailed research due to their size, complexity and security and quality requirements. These projects have been studied in greater detail, with further data being collected from numerous interviews, observations and project documentation over a 6-12 month period for each project. Action research was the research methodology chosen as the researcher was directly involved in the process and outcomes of all four projects. Action research involves taking part in the action and using the involvement in the change process as a research experience (Checkland and Poulter, 2006). This paper presents only an overview of the four cases to highlight the problems faced in the chosen situations. Development of a model for late intervention in such projects is still in progress.

3. IT Security and Quality: Scoping the Problem

The four cases presented cover various industries, budgets, team size, operating models and geographical locations. The projects are different in nature and each represents a unique case impacted by it is environments and the people working on it. These consequently affect the project outcomes including the security and quality requirements.

3.1. Case 1 (Power Utility Company)

The first company investigated was a large power utility company, employing 600 staff. The Information Systems department had 60 staff, most of them contractors working on various projects. Application development and support was outsourced to a foreign vendor, whilst the infrastructure management was outsourced to a local vendor. The project was initiated and driven by a master plan managed by the previous owner. The driver for this project was the result of the previous owner's declaration that it no longer wished to provide IT services to the newly formed company. The company decided 6 months later that it would not be part of the previous owner led separation program, but instead it would establish its own separation and sourcing efforts due to changes in the company internal IT priorities. The company also recognised that this effort required significant involvement from the previous owner's internal resources. The company established its own separation project and a parallel sourcing project to engage external vendors to support the IT department. These projects were tightly linked, with a number of cross dependencies. The separation project was managed as a strategic IT effort, whereas the sourcing project was considered business transformation. The separation in the context of the project meant moving applications hosted by the parent company to a newly established hardware platform within the company. The project suffered from having a low profile within the company, and had attracted a negative reputation for running overtime with no definite end date. The operations department did not fully support the project as they did not recognise the benefits, increased efficiency or productivity. The business had seen many changes to its operating model which had resulted in the loss of a significant number of experienced staff. The company went through multiple rounds of restructuring that affected the project team, with 3 project managers changing hands in one calendar year. The company had a unique mix of staff with less than 40% of the staff being permanent, while the rest were contractors engaged with the company for limited durations, varying from 3 to 6 months.

The separation project had 23 major applications within its scope, 10 of these applications had been classified with business critical impact. One application within the scope was used to process a very large amount of bill payments from customers on an annual basis. The bill payment application had been in production for 9 years, hosted by the parent company. Two weeks prior to the go live date, the operation department highlighted the need to conduct penetration testing and code review on the application as a condition for sign off. The initial response from the project manager was "the application has been in operation for so long and no functional changes have been made. Going through the process of procuring and conducting the required test will impact the project timeline". With deadlines approaching, the project manager reluctantly accepted performing the penetration testing and code review. The penetration testing of the application led to the following key findings:

- The application was vulnerable to cross-site request forgery, potentially allowing attackers to execute actions on behalf of legitimate users.
- The application did not limit the amount of submission attempts made to webforms, allowing an attacker to launch a brute force attack to discover valid input.
- The application had been designed using a two stage http post request, allowing an attacker to bypass any input checks and controls integrated into the application.
- The intrusion prevention system (IPS) in place did not appear to inspect https traffic, allowing an attacker to proceed attacking the web server uninhibited by IPS filters.

It is also important to highlight that the company network infrastructure team submitted earlier recommendation, to deploy multiple intrusion detection systems as well as an application layer firewall installed on the application server to ensure the security in depth principle was applied to sensitive applications. The proposal was not accepted by the operations department due to budgetary constraints. The operations department's response to the penetration test report was "in terms of recommendations from operational security, we are in a position where I think we can move the application into production as scheduled" (Officer, 2010).

In summary, the project suffered from political and structural difficulties from its inception. The value of the project was not fully known and appreciated by key decision-makers and the project champion did not appear to be fully committed to the project. Short-term contracts for the hire of external contractors lead to a high turnover of staff resulting in a lack of ownership. Security and quality of the application were identified as concerns prior to going live. Penetration testing findings highlighted gaps in the application logic, as well a number of design flaws that would allow experienced hackers to damage the payment gateway resulting in organisational reputation damage. However, the application went live as scheduled despite the identified risks.

3.2. Case 2 (Federal Government Initiative)

The second case study was a project within a large federal government department, employing 10 external IT contractors and a budget of $4 million. The project is a national vision to transform paper-based processes into an electronic format that would be efficient and able to meet the needs of those involved in the development of land and dwellings assessments. The project was tasked to create and maintain a national communication protocol that could be use by all states and territories.

Stakeholders in the area of land development area recognised problems with the existing manual system that affected land available for development. Whilst the primary focus of the initiatives was to streamline business processes related to land development assessment processes, a valuable by-product of taking the assessment process online was to automate the lodgement of development applications which would increase the process performance and further reduce the cost incurred by developers. The overall scope of the project was to develop a national communication protocol suitable for use by proponents and regulators in all states and territories that:

- Used the extensible Markup Language (XML) supported by agreed non-proprietary formats (file types) for submitted plans and documents;
- Developed XML schema compliant with the interoperability technical framework published by the national government;
- Focused on enabling existing systems and processes to communicate rather than developing new procedures; and
- Provided a framework flexible enough to allow other relevant application types to be included at a later date.

The project provided details on how an XML standard might be implemented, managed and adopted. The development of applications using the model or recommendations regarding the tools or mechanisms used to transfer data, and the process to map data to agencies' own systems was out of the scope of this project. The development of the protocol has suffered from many setbacks during the project timeline, including:

- The company responsible for building conformance test harness went out of business, with no recoverable intellectual property that could aid the project.
- There was no central authority responsible for the project deliverables.
- There were conflicting jurisdictional requirements and an inability to agree on some key definitions and requirements.

Following a prolonged timeline a national coordination office was established with the mission to ensure project outcomes defined by the stakeholders was achieved. With the coordination office in place, the protocol went through a process of clarification that resulted in an agreed format for the protocol, and a project team was formed to build a conformance platform that would be used by states and territories to conform with the protocol. The protocol design suffered some fundamental problems that were introduced in an attempt to gain the agreement from the various stakeholders. These were:

- The UML model did not specify any security method to secure data transmission and storage;
- The jurisdiction did not agree to implement digital certificates as they were deemed of no business value;
- The application that to be used by states and territories to comply with the national protocol did not have any requirements for security other than the Username/Password implemented using an open source tool.

Unfortunately security considerations and features remain limited or non-existent in the national platform. In addition some assumptions were made by a number of project members; including:

- The project did not mandate technology solutions, it only provided the framework.
- No security requirements were included in the scope of the project;
- Security would be implemented as part of each jurisdiction's special implementation of the protocol;
- If security was implemented, the project would suffer from delays that would affect funding availability (milestone = funding);
- A new version of the protocol would be needed if any security mechanism was adopted, which would require the protocol to go through a long review process and certification from the relevant agencies.

In summary, with limited ownership of the final delivery, the initiative suffered from prolonged delays to realise its promised benefits. Whilst stakeholders provided the project requirements, they were inaccurate and ambiguous which hindered the initiative progress until national coordination office is established. Stakeholders placed limited or no emphasises on security and quality risks due to lack of explicit security and quality requirements. The project's longer term objectives were jeopardised due to the reliance upon external contractors with no long term plan for knowledge retention. The initiative lacked the typical project governance structure that traditionally used to guide projects, namely project planning, and budget and scope management.

3.3. Case 3 (Stock Exchange)

The stock exchange studied was one the largest in Asia with 450 full time employees. The exchange had an internal technology department that employed 20 project managers and business analysts who worked on different projects. Infrastructure management was outsourced to a global service provider, and had no internal testing capability. The exchange selected an international software provider as the preferred supplier for both an upgraded derivatives trading platform and a new derivatives settlement system to replace existing settlement systems that was used to transfer ownership of shares and options traded in the exchange. As part of the upgrade process the vendor was required to enhance their data engine product to support new data storage requirements. Enhancements and software upgrades were also required for many other internal systems which sent and received data from the settlement system.

The stock exchange outsourced the quality assurance element of the project to a third party, who in turn recruited industry professionals. Many of the staff recruited for the project had no experience in quality assurance (QA) or in financial applications. The project had 80 staff dedicated to quality assurance, supported by a number of Subject Matter Experts and Business Analysts, as well as onsite vendor support. The project had very strict deadlines that were communicated to the market, and any changes to the go live date presented a reputational risk to the exchange. Part of the project was the deployment of twelve different sub-systems that supported the settlement system, including pricing, risk assessment, and payment applications, as well as an interface to trade with other exchanges around the world. The QA component of the project represented approximately 75% of the entire project timeline, and the QA scope increased with the finding of more critical defects. Penetration testing was part of the QA scope and was performed by large consulting firms. Some of the issues faced during the penetration execution were:

- Ten working days were allocated for the penetration test, with three days lost while trying to secure access to the exchange testing platform to the consultancy firm performing the penetration testing, due to delayed approval from the exchange's head of IT security.
- Penetration testing shared the same platform with functional testing, which required putting constraints on the types of testing allowed by the consultancy firm performing the penetration testing. Functional testing ranked higher on the priority list for the project.

- The environment configuration used to perform the penetration testing did not match the actual production system, and had no security applications installed except the basic username/password requirements.
- None of the applications had any specific security requirements except integration with the exchange's Active Directory platform.

The findings of the penetration test presented concerns for the project, with 70 issues identified; many of them critical (mainly design flaws). The developers of the sub-systems objected to the penetration test results, and argued that the signed-off requirements documents included no security requirements. Most of the findings were dismissed by upper management (at the CIO level), with the direction that focus must remain to the commitment to go live on the date announced to the market. The sub-system developers were asked to address 10 issues that were deemed important by the operations department and the remaining 60 issues to be addressed in the future with no specified date.

In summary quality assurance and security testing was planned as part of the overall project plan. Quality assurance suffered from frequent changes to the agreed scope, reliance of inexperienced staff to perform the planned testing activities .The organisation had some consideration for security, evidenced by the inclusion of penetration testing as part of the QA scope. However, the execution and final outcome of the penetration testing highlighted no willingness from the organisation to consider the overall security of the deployed applications.

3.4. Case 4 (State Government Department)

The department worked with the community to ensure high standards of safety and protection of consumers, and promotes and fostered innovative industries, science and enterprise. The department had various IT divisions, including a project management office that employed approximately 40 staff, 90% of them being contractors (Project Managers, Business Analysts, and Architects). The department also had a separate IT division responsible for managing infrastructure, and call centres to handle internal and external support inquires. This project aimed to modify the existing complaints and licensing system to accommodate licensing, certification and registration processes and to facilitate new licences from various divisions. The project planned to significantly enhance and deliver improved usability, performance and general functionality to existing users with no interruption to normal operations. Web-enabled aspects of licensing such as application, renewal payments, enquiries and self-service functionality were part of the overall project scope, with a number of existing systems to be decommissioned. The application was developed using legacy technology that is no longer supported by the vendor, the enhanced system planned to be developed using the same legacy technology. One of the project objectives was to overhaul the existing security model. The original application security was limited to user name/password and group that defined the department to which a staff member belonged in addition to his/her position (staff, supervisor and manager). The model did not have sufficient granularity to limit who could view licensing details of various departments, highlighted by the fact that a supervisor could see other supervisor's work and approve them. One of the project's main success criteria as defined in the project initiation document was the successful implementation of a new security model that would meet the business needs. The project suffered from many issues that affected its deliverables:

- Limited availability of staff familiar with the legacy technology;
- No staff were allocated to test the application;
- There was difficulty obtaining agreement from the business divisions on what constituted security and general quality acceptance criteria;
- The IT section was perceived to be dictating to the business how the application would be implemented and used;
- There was limited planning at the early stages of the project resulting in significant effort underestimating (e.g. staffing) and budget requirements.

The original planning led to underestimation of the security requirements and with a stretched project timeline, the security requirements were deemed excessive and went through various revisions. It was necessary for the IT group to simplify the security requirements and present cheaper options to the business. The new security model required features where one or many system users could be assigned to particular licence type and staff roles performing tasks on particular licences restricted to their access level and their work duties. The security model was deemed insufficient by the business, as it only added one new layer of granularity to split the users amongst the various divisions, with each division having one or more supervisors with one or many reporting staff. However, the business and the IT section finally agreed on the design with minor changes to the refined security model that addressed some of the business concerns. Another challenge faced by the project was the lack of QA staff. The project went through the planning, design, and 6 phases of implementation with no QA staff to verify the quality of the products that had been implemented. It was agreed earlier by stakeholders that the business would have sufficient staff to address all quality assurance requirements of the project. As the project progressed it became apparent that the business would not be able to provide the necessary staff to support the QA effort. The project had to turn to the market to recruit at least one staff to support the testing requirements of the project.

The project engaged external QA consultants on a part-time basis to train internal non-IT staff and drive the QA effort for several months. This allowed the project to establish a QA framework in an attempt to improve the quality assurance approach employed by the project to date, which relied on the developers to conduct limited functional testing, but no unit testing as it was viewed as excessive by the development team. The department employed PRINCE2 methodology for project management, Rational Unified Process (RUP) as the development methodology, and ITIL for Service Delivery. The department's IT Governance section made recommendations to include provisions of testing from the beginning of the project to minimise risks associated with project delivery. The project went live twelve months late with no quality assurance staff supporting the project effort.

In summary, the security scope of the application was underestimated which lead to delayed project delivery. Quality assurance suffered due to the business stakeholder's inability to provide the necessary staff to carry out the planned testing activities. Despite the fact that the project engaged an external QA consultant, it was only for short period of time. This limited the scope of the application testing being undertaken. Whilst the department employed methodologies to control the project and its deliveries, the project was late, over budget and didn't employ the department's own IT governance guidelines with regard to the inclusion of testing at early stages of the project.

4. Common Emergent Themes across the Case Studies

Common problems emerge from the analyses of these case situations:

- Slow or no reaction to emerging signs of problems in projects. This has the potential to limit the ability of projects to be successful or deliver their intended outcomes.
- Lack of defined security requirements and strict quality assurance procedures. This can results in either lack or limited implementation of security measures built in to the applications, whilst dealing with quality assurance as afterthought results in expensive applications maintenance post go live.
- Inconsistent application of project management, development, and internal methodologies and guidelines. The implications of this include the increased risk of not meeting project requirements, missing critical tasks and features, and project over-runs in time and cost.
- Inadequate planning of projects, resources, and staffing requirements. This could result in change requests being raised to address the frequent changes to scope and staffing requirements, consequently increasing the project budget and timeline.
- Reliance on contracting and outsourcing agreements, and lack of investment in knowledge retention, training, and skills. The short-term approach of using contractors and outsourcing may have the lure of monetary saving, however it also has the potential to leave organisations unable to cope with unexpected events, as they don't have the resources or knowledge in-house to cope.
- Lack of involvement by senior decision-makers in the change management process that directly affects security and quality issues. Without quality and security champions in the organisations projects may still be delivered, but risk-finding and fixing security and quality issues whilst in production will be costly and could negatively impact the organization's future operations.
- The gap between Strategic Planning and Project Management where the strategies do not directly address the major issues associated with IT projects (e.g. resource allocations, project sponsorship, project profile). This lack of integration presents a gap which has the potential to deliver inadequate return on investment made in information technology.

5. Conclusion

Two prominent issues in the case studies relate to limited or lack of security and quality requirements during the early stages of a project and the lack of planning and management of security and quality requirements as the projects progress. Existing security and quality models promote addressing security and quality issues early in the project life cycle, and while this is the preferred approach, it is not always the case in practice. Every IT project is unique and there are many internal and external factors that affect a project's ability to deliver all agreed requirements, while attempting to address security and quality concerns. This problem is a complex one with no easy solution. Two alternatives come to mind: first, senior managers actually follow the traditional models that require security and quality concerns to be addressed early in the project lifecycle. Alternatively if project managers and senior decision-makers continue to disregard security and quality issues perhaps an intervention model is required to address the implications of time and cost over-runs toward the end of the project. Such a model for late intervention would need to be designed to weigh up the implications of poor specification and delayed action, i.e. the costs in time, money and reputation.

6. References

Borenstein, N (1991), "Programming as if people mattered: Friendly programs, Software engineering, and other noble delusions", Princeton University Press, Princeton, New Jersey.

Checkland, P. & Poulter, J (2006), "Learning for Action", John Wiley & Sons Ltd, West Sussex, England

Denning, P (1990), "Computers Under Attack: Intruders, Worms and Viruses", Addison Wesley, New York

Leveson, NG & Turner, CS (1993), "An Investigation of the Therac-25 Accidents", Computer, vol. 26, no. 7, pp. 18-41.

Neumann, P (1995), "Computer Related Risks", Addison-Wesley, New York

Officer, IS (2010), "Penetration Test Report", ed. HE Desouki, p. 2, 21/01/2010.

Technology, NIoSa (2006), "Requiring Software Independence in VVSG 2007: STS Recommendations for the TGDC", 1 December 2006. Retrieved 8/02/2010, from http://vote.nist.gov/DraftWhitePaperOnSIinVVSG2007-20061120.pdf

Valdes-Dapena, P & Lah, K (2010), "Toyota: Software to blame for Prius brake problems", CNN, 4/02/2010 Retrieved 9/02/2010, from http://www.cnn.com/2010/WORLD/asiapcf/02/04/japan.prius.complaints/index.html

Woodward, M & Hennell, M (2005), "Strategic benefits of software test management: a case study", Journal of Engineering and Technology Management, vol. 22, no. 1-2, pp. 113-40.