Abstract: The paper focus on the main key points related to the IT security project management. The most important lifecycle stages are identified: IT security project proposal definition, project organization, project planning, quality planning, project team organization, IT security project activities management and project closing. The most important success factors for IT security projects are the support of top-management, customer satisfaction, prevention over remediation and continuous progress. Also, the project manager skills are highlighted in this specific context.

Key-Words: IT security projects, project management, quality, metrics, project lifecycle, security threats

1. Introduction

IT security projects are required in almost every area of software development. These projects can be found from mobile applications to complex collaborative systems. The success or failure of these projects is influenced by the associated project management process. In order to be successful, the IT security projects require a very good project management process that has to be adapted to their specific characteristics. The paper aims to highlight, from the project management perspective, the success factors for IT security projects.

The paper is structured as follows. The section IT Security Project Management focuses on project management aspects related to projects that involves IT security.

The section IT Security Related Projects deals with examples of such projects and their main characteristics.

In the last section entitled IT Security Projects Metrics are presented several factors that influence the metrics for these types of projects. The factors are related to personnel, process and product.

The paper ends with conclusions and future work.

2. IT Security Project Management

Project Management becomes a real challenge for the enterprise wide IT security projects, so the question that appears here is how to properly manage such a project? Is there a way to adapt the project management principles for this sensitive field called enterprise security?

The starting idea could be the PMI’s point of view related to the way in which projects from various fields could be managed. The theory states that any project should use the same project management methodology (also called process), since the methodology is industry independent [3]. By looking the things from this perspective, any enterprise wide IT security project will cover the five project management process groups (Figure1):

- **Initiating** – based on the high-level planning completed at this level, it could be decided the project will be selected to be accomplished
- **Planning** – the detailed project management plans are developed
- **Executing** – performing the work to be done according to the plans
- **Monitoring and Controlling** – verify the project is on the track in terms of scope, time, cost, risk and quality
• **Closing** – make sure all the work is completed according to the plans and the project met the objectives stated into the project management plans.

The project management process groups can only be applied together with a progression of phases that are industry dependent called *project lifecycle*, so projects from various fields will implement different stages (generally sequential).

Small projects typically use a single set of project management process groups, as illustrated in Figure 1.

![Figure 1. Project Management Process Groups for Small Projects](image1)

Large projects are usually divided into phases, each phase having its own set of project management process groups, Figure 2.

![Figure 2. Project Management Process Groups for Large Projects](image2)

Today, it becomes very clear the project management influence is crucial for IT security projects of the following areas:

• Information Governance
• Knowledge Management
• Information Assurance
• Informal social networks
• Security Portfolio Management

In this context of IT security projects, the skills of the project manager are very important and should include at least the following items:

• A very good understanding of the technology and industry
• IT security focus
• Understand the project attributes, like goals, constraints, lifecycle, conditions, and limitations
• Contribution of organizational structure, culture and assets to the success of a IT security project
• Relevant experience, both in project management and IT security
A string project management methodology to be used
- Personal qualities, like communication skills, problem solving capabilities and a very creative thinker mind
- Vision is needed for the project manager to design a customized solution to solve the security issues reported by the project stakeholders since general approaches are not working in this sensitive field
- Economic background is very useful since most project selection methods are based on financial projections of the project monetary data

Usually, the projects in the IT security field are facing various limiting factors. The most relevant are illustrated by the Iron Hexagon (Figure 3), where [9]:
- Schedule – time needed to deliver the IT security project
- Risk – threats and opportunities
- Scope – what has to be done, the boundaries of the IT security project
- Resources – project team that is developing and delivering the security project
- Cost – the amount of money needed to complete the project
- Quality – the project must meet at least some minimal functional and non functional requirements related to quality attributes. The changes that can be usually assumed are corrective actions (improve the performance in the near future), preventive actions (reduce the probability of negative consequences) and defect repair (actually means repairing or replacing the product). There are two main types of quality costs, cost of good quality (costs related to conformance in order to avoid the failures) and - cost of poor quality (costs related to nonconformance).

Related to the IT security issues, the most exposed companies are the ones that are dropping under at least one of the following categories [2]:
- Cloud oriented applications or Internet based platforms – the more a company depends on the Internet, the greater becomes the need of security in order to avoid activity interruptions, data losses, legislation violation of the personal information that is confidential by law;
- Employees are working in virtual teams with members located in different places – increased security demands required by the need of full remote access to the company resources;
- E-commerce and e-business solutions – the transactions should be secured, the electronic payments must be safe, the user personal information should remain confidential, the relationships with the traditional business partners could be tremendously affected by any security problems that might appear;
- Data transfer over the network – many companies are transferring sensitive data from one location to another, such transfers are rising
huge security risks, even if secured and dedicated technologies are used;

- **Manipulation of sensitive data** – the privacy of some personal information is legally enforced, so any security issue in this area can lead to legal conflicts and financial penalties.

### 3. IT Security Related Projects

A typical IT security related project usually involves the following lifecycle stages, based on [1]:

- **Defining the IT security project proposal** – including identifying the potential security problems and appropriate solutions, finding the optimal security approaches, defining the high-level constraints (iron triangle – scope, time, cost and quality – Figure 4), identifying the main project stakeholders and sponsors;

![Figure 4. The Iron Triangle (Triple Constraint)](image)

- **Organizing the project** – including defining the requirements, scope, acceptance criteria and CCB (Change Control Board) organization rules, refining the project scope and related objectives; an iterative clarification of the high level customer needs also takes place at this stage, including but not limited to the project justification, objectives, high level requirements, summary budget, milestones and risks. All these elements become part of the *project charter*;

- **Project planning** – defining the activities, sequencing these activities, estimations for the durations and resources needed, generating the project schedule, dealing with the project constraints related to budget, scope, time, cost, quality; if needed, fast tracking or crashing scenarios should be defined to be applied later. The analysis part starts by identifying the scope of the project and the actions to be performed in order to meet the requirements, so approved *project management plans* will be available including requirements refinement, scope definition, WBS creation, project schedule, cost and budget estimations, quality requirements, risk identifications and response planning;

- **Quality planning** – including the definition of requirements (functional, non-functional, technical constraints), quality metrics, acceptance criteria, CM (Change Management) procedures, test plans and test cases [6]. Also, the continuous quality monitoring and controlling is very important to be planned at this stage; quality plays an important role for any project success;

- **Organizing the project team** – defining the team requirements, roles, responsibilities, constraints, motivating and training needs; project management plans should be developed in order to acquire, develop and manage the project team during the project life cycle;

- **Managing the IT security project activities** – monitoring the project progress, issue tracking, defect reporting, creating the documentation, taking into account
the project risks, perform risk reassessment on a regular basis, configuration management and change control, fast tracking, crashing, testing the project results, etc. In order to measure the potential deviation of project performance in terms of schedule and costs, the EVM (Earned Value Measurement) method is usually applied. EVM is based on the following three points that need to be computed on a regular basis [4]:

- \( EV \) (Earned Value – estimated value of the work already accomplished) – this data is measured by collecting the % progress from the project team and applying it to the total estimated efforts
- \( PV \) (Planned Value – estimated value of the work planned to be done) – this is generated directly from the project plan file by using dedicated tool
- \( AC \) (Actual Cost – the cost of the work accomplished) – this is taken from the Work Tracking System, the value is based on the daily reporting of the project team

The Schedule Variance (SV), Schedule Performance Index (SPI), Cost Variance (CV) and Cost Performance Index (CPI) are measuring the project deviations in terms of schedule and costs so these indicators can be used to point out if the project is still on the track. Also, EAC (Estimate At Completion), ETC (Estimate To Complete) and VAC (Variance At Completion) are other additional useful EVM indicators.

4. IT Security Projects Metrics

In [5] are presented the factors that can be measured and used in IT project management metrics. These factors are classified in: personnel, process and project/project indicators. Based on this classification, these factors are adapted for IT security projects. For IT security project, the personnel evaluation will take into account the following:

- Education level (degrees, certifications, courses etc.);
- Degree of confidence;
- Previous experience;
- Social and communication abilities;
- Team members homogeneity;
- Personnel productivity;
- Certification level.

Another important issue refers to the quality of training and education on project management, this being analyzed in [10].

The process evaluation focuses on the maturity of the IT project management. High quality of project deliverables cannot be obtained without a high quality process. That does not guarantee that quality products will be obtained. The quality of the process is certified through general and specific quality standards. The following factors are used to evaluate the process:

- Development techniques and methodologies;
The company level of certification (regarding security, project management, software development, quality management);
- The software and hardware degree of novelty;
- Programming languages, frameworks and technologies used;
- The degree of reuse (software, procedures etc.);
- The audit processes results;
- Security.

Some factors derive from the product/project characteristics and its related environment. There are several factors related to the project/product evaluation, like:
- Security standards (internal and external);
- Required level of confidence;
- Number of users and stakeholders;
- Project and product complexity;
- The existence of similar product on the market;
- Application specific (required level of security, reliability etc.).

Some of the most important project management metrics related to IT security projects are presented in table 1. These metrics are using [5] as starting point.

<table>
<thead>
<tr>
<th>Category</th>
<th>Metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process</td>
<td>Number of security procedures</td>
</tr>
<tr>
<td></td>
<td>Number of security tests</td>
</tr>
<tr>
<td>Quality</td>
<td>Project complexity</td>
</tr>
<tr>
<td></td>
<td>The degree of client/executive management/stakeholders satisfaction</td>
</tr>
<tr>
<td></td>
<td>Number of complaints due to security issues</td>
</tr>
<tr>
<td></td>
<td>Portfolio complexity</td>
</tr>
<tr>
<td></td>
<td>Number of security failures (testing)</td>
</tr>
<tr>
<td>Costs</td>
<td>Cost of security</td>
</tr>
<tr>
<td></td>
<td>Cost of non-security</td>
</tr>
<tr>
<td></td>
<td>Statistics regarding different costs categories</td>
</tr>
<tr>
<td></td>
<td>Project portfolio value</td>
</tr>
<tr>
<td>Personnel</td>
<td>Number of certified people</td>
</tr>
<tr>
<td></td>
<td>Degree of confidence</td>
</tr>
<tr>
<td></td>
<td>Work productivity</td>
</tr>
<tr>
<td></td>
<td>Experience in security projects (years/months)</td>
</tr>
<tr>
<td>Product</td>
<td>Number of security requirements</td>
</tr>
<tr>
<td></td>
<td>Number of security characteristics</td>
</tr>
<tr>
<td></td>
<td>Number of encryption/decryption algorithms used</td>
</tr>
</tbody>
</table>

Depending on the project complexity, the security aspects that have to be taken into account varies. For example, collaborative systems, that require a high level of security, have numerous integrated metrics and indicators, as stated in [7].

The metrics have to be tested and validated after they will be used in practice. Also, the metrics have to be integrated in a system in order to assure a high level of confidence in company and its products and services.

5. Conclusions and Future Work

Based on the lifecycle stages described above, we can conclude the success of any IT security project is strictly related to the following sensitive areas:
- Since security is one of the top-management responsibilities, any IT security project needs the appropriate resources to be available when necessary, so the support of executives is really mandatory;
Customer satisfaction is vital – the customer requirements should be completely met at the highest quality level possible;

Prevention over remediation – the modern approaches are stating the security is designed and built in, not remediated since the costs of prevention are much lower than the efforts needed to fix a security breach;

Continuous progress – the security level and quality should increase in time, from one project to another.

The next steps will be to develop and validate these metrics in order to build an integrated metrics system for IT project management.

References